K H Spencer Pickett

The internal auditing HANDBOOK

Third Edition

THE INTERNAL AUDITING HANDBOOK

THE INTERNAL AUDITING HANDBOOK

Third edition

K. H. Spencer Pickett

(Assisted by Jennifer M. Pickett)

WILEY

A John Wiley and Sons, Ltd., Publication

Copyright © 2010 K.H. Spencer Pickett

Registered office
John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom

For details of our global editorial offices, for customer services and for information about how to apply for permission to reuse the copyright material in this book please see our website at www.wiley.com

The right of the author to be identified as the author of this work has been asserted in accordance with the Copyright, Designs and Patents Act 1988.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, except as permitted by the UK Copyright, Designs and Patents Act 1988, without the prior permission of the publisher.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

Designations used by companies to distinguish their products are often claimed as trademarks. All brand names and product names used in this book are trade names, service marks, trademarks or registered trademarks of their respective owners. The publisher is not associated with any product or vendor mentioned in this book. This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold on the understanding that the publisher is not engaged in rendering professional services. If professional advice or other expert assistance is required, the services of a competent professional should be sought.

Library of Congress Cataloging-in-Publication Data

Pickett, K. H. Spencer.
The internal auditing handbook / K.H. Spencer Pickett. – 3rd ed.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-470-51871-7
1. Auditing, Internal. I. Title.
HF5668.25.P53 2010
657′.458 – dc22

2010004323

ISBN 978-0-470-51871-7

A catalogue record for this book is available from the British Library.

Typeset in 9.5/12 Gill Sans Light by Laserwords Private Limited, Chennai, India.
Printed in Great Britain by CPI Antony Rowe, Chippenham, Wiltshire.

This handbook is dedicated to the memory of my mother, Joycelyn, who passed away in August 2002

CONTENTS

List of Abbreviations xi
Foreword to Second Edition xv
Acknowledgements xvii

1 Introduction 1
Introduction 1
1.1 Reasoning behind the Book 2
1.2 The IIA Standards and Links to the Book 3
1.3 How to Navigate around the Book 4
1.4 The Handbook as a Development Tool 7
1.5 The Development of Internal Auditing 7
Summary and Conclusions 19
References 21

2 Corporate Governance Perspectives 23
Introduction 23
2.1 The Agency Concept 24
2.2 Corporate Ethics and Accountability 29
2.3 International Scandals and their Impact 39
2.4 Models of Corporate Governance 47
2.5 Putting Governance into Practice 73
2.6 The External Audit 87
2.7 The Audit Committee 120
2.8 Internal Audit 136
2.9 The Link to Risk Management and Internal Control 141
2.10 Reporting on Internal Controls 142
2.11 New Developments 146
Summary and Conclusions 159
Assignment Questions 161
Multi-choice Questions 161
References 168

3 Managing Risk 173
Introduction 173
3.1 What Is Risk? 175
3.2 The Risk Challenge 176
3.3 Risk Management and Residual Risk 179
3.4 Mitigation through Controls 182
3.5 Risk Registers and Appetites 186
3.6 The Risk Policy 192

	3.7	Enterprise-wide Risk Management	203
	3.8	Control Self-assessment	213
	3.9	Embedded Risk Management	218
	3.10	The Internal Audit Role in Risk Management	221
	3.11	New Developments	230
		Summary and Conclusions	236
		Assignment Questions	237
		Multi-choice Questions	238
		References	242
4	Internal Controls		245
		Introduction	245
	4.1	Why Controls?	245
	4.2	Control Framework – COSO	255
	4.3	Control Framework – CoCo	264
	4.4	Other Control Models	267
	4.5	Links to Risk Management	272
	4.6	Control Mechanisms	274
	4.7	Importance of Procedures	285
	4.8	Integrating Controls	287
	4.9	The Fallacy of Perfection	289
	4.10	Internal Control Awareness Training	292
	4.11	New Developments	299
		Summary and Conclusions	301
		Assignment Questions	302
		Multi-choice Questions	303
		References	309
5	The Internal Audit Role		311
		Introduction	311
	5.1	Why Auditing?	311
	5.2	Defining Internal Audit	313
	5.3	The Audit Charter	325
	5.4	Audit Services	334
	5.5	Independence	340
	5.6	Audit Ethics	355
	5.7	Police Officer versus Consultant	363
	5.8	Managing Expectations through Web Design	382
	5.9	Audit Competencies	386
	5.10	Training and Development	393
	5.11	New Developments	403
		Summary and Conclusions	410
		Assignment Questions	412
		Multi-choice Questions	412
		References	420
6	Professionalism		421
		Introduction	421

	6.1	Audit Professionalism	421
	6.2	Internal Auditing Standards	429
	6.3	Due Professional Care	453
	6.4	Professional Consulting Services	457
	6.5	The Quality Concept	459
	6.6	Defining the Client	469
	6.7	Internal Review and External Review	470
	6.8	Tools and Techniques	478
	6.9	Marketing the Audit Role	483
	6.10	Continuous Improvement	491
	6.11	New Developments	494
		Summary and Conclusions	495
		Assignment Questions	497
		Multi-choice Questions	497
		References	502
7	The Audit Approach		505
		Introduction	505
	7.1	The Systems Approach	506
	7.2	Control Risk Self-assessment (CRSA)	523
	7.3	Facilitation Skills	531
	7.4	Integrating Self-assessment and Audit	539
	7.5	Fraud Investigations	543
	7.6	Information Systems Auditing	586
	7.7	Compliance	636
	7.8	VFM, Social and Financial Audits	642
	7.9	The Consulting Approach	653
	7.10	The 'Right' Structure	669
	7.11	New Developments	675
		Summary and Conclusions	677
		Assignment Questions	677
		Multi-choice Questions	678
		References	694
8	Setting an Audit Strategy		697
		Introduction	697
	8.1	Risk-based Strategic Planning	698
	8.2	Resourcing the Strategy	714
	8.3	Managing Performance	722
	8.4	Dealing with Typical Problems	737
	8.5	The Audit Manual	745
	8.6	Delegating Audit Work	758
	8.7	Audit Information Systems	761
	8.8	Establishing a New Internal Audit Shop	771
	8.9	The Outsourcing Approach	778
	8.10	The Audit Planning Process	789
	8.11	New Developments	802
		Summary and Conclusions	807

		Assignment Questions	810
		Multi-choice Questions	811
		References	825
9	Audit Field Work		827
		Introduction	827
	9.1	Planning the Audit	827
	9.2	Interviewing Skills	839
	9.3	Ascertaining the System	858
	9.4	Evaluation	864
	9.5	Testing Strategies	877
	9.6	Evidence and Working Papers	896
	9.7	Statistical Sampling	909
	9.8	Reporting Results of the Audit	920
	9.9	Formal Presentations	953
	9.10	Audit Committee Reporting	960
	9.11	New Developments	964
		Summary and Conclusions	970
		Assignment Questions	973
		Multi-choice Questions	974
		References	1006
10	Meeting the Challenge		1009
		Introduction	1009
	10.1	The New Dimensions of Internal Auditing	1009
	10.2	The Audit Reputation	1010
	10.3	Globalization	1012
	10.4	Examples	1014
	10.5	Meeting the Challenge	1015
		Summary and Conclusions	1023
		Multi-choice Questions	1024
		References	1025
Appendix A	Induction/Orientation Programme		1027
Appendix B	CRSA Best Practice Guide		1029
Appendix C	A Poem by Professor Gerald Vinten		1033
Appendix D	Analytical Techniques by Sue Seamour		1037
Appendix E	Multi-choice Questions: Answer Guide		1041
Index			1057

LIST OF ABBREVIATIONS

AC	Audit Committee
ACCA	Association of Chartered Certified Accountants
ACR	Assurance, Control and Risk
AIB	Allied Irish Bank
AICPA	American Institute of Certified Public Accountants
AIRMIC	Association of Insurance and Risk Managers
ALARM	Association of Local Authority Risk Managers
AO	Accounting Officer
APB	Auditing Practices Board
BA	Business Area
BBC	British Broadcasting Corporation
BCCI	Bank of Credit and Commerce International
BCP	Business Continuity Program
BFS	Baring Futures Singapore
BV	Book Value
C&AG	Comptroller and Auditor General
CAAT	Computer Assisted Audit Techniques
CAE	Chief Audit Executive
CBI	Confederation of British Industry
CBOK	Common Body of Knowledge
CCAB	Consultative Committee of Accountancy Bodies
CEO	Chief Executive Officer
CFIA	Competency Framework for Internal Auditors
CFO	Chief Financial Officer
CG	Corporate Governance
CIA	Chief Internal Auditor
CICA	Canadian Institute of Chartered Accountants
CIMA	Chartered Institute of Management Accountants
CIO	Chief Information Officer
CIPFA	Chartered Institute of Public Finance and Accountancy
CISO	Chief Information Security Officer
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CPA	Certified Public Accountant
CPD	Continuing Professional Development
CPE	Continuing Professional Education
CRO	Chief Risk Officer
CRSA	Control and Risk Self-Assessment
CSA	Control Self-Assessment
CSFB	Credit Suisse First Boston

CSI	Computer Security Institute
CSR	Corporate Social Responsibility
DA	District Auditor
DF	Director of Finance
DGIA	Directorate General for Internal Audit
DP	Data Protection
DR	Disaster Recovery
DRP	Disaster-Recovery Program
DTI	Department of Trade and Industry
EA	External Audit
EC	European Commission
ECIIA	European Confederation of Institutes of Internal Auditing
EFQM	European Foundation Quality Model
ERM	Enterprise Risk Management
ERM	Effective Risk Management
EU	European Union
FCO	Foreign and Commonwealth Office
FD	Finance Director
FEI	Financial Executives International
FRC	Financial Reporting Council
FRRP	Financial Reporting Review Panel
FSA	Financial Services Authority
GAAP	Generally Accepted Accounting Policies
GAIN	Global Audit Information Network
GAO	Government Accountability Office
GAP	Generally Accepted Accounting Principles
GAR	Guaranteed Annuity Rate
GRC	Governance, Risk, and Control
GSE	Government-Sponsored Enterprises
HM	Her Majesty's
HoP	Head of Personnel
HR	Human Resource
HRM	Human Resource Management
IA	Internal Audit
IC	Input Control
ICAEW	Institute of Chartered Accountants in England and Wales
ICE	Internal Control Evaluation
ICGN	International Corporate Governance Network
ICQ	Internal Control Questionnaire
IFRS	International Financial Reporting Standards
IIA	Institute of Internal Auditors
IiP	Investors in People
IMC	Institute of Management Consultants
IoD	Institute of Directors
IPPF	International Professional Practices Framework
IPSAS	International Public Sector Accounting Standards
IRC	INFOSEC Research Council
IS	Information Systems

ISO	International Standards Organization
ISS	Institutional Shareholder Services
IT	Information Technology
JDS	Joint Disciplinary Scheme
KPIs	Key Performance Indicators
KPMG	Klynveld, Peat, Main and Goerdeler
KRCM	Key Risk and Control Matrix
MIIA	Advanced Diploma in Internal Audit Management
MIS	Management Information System
MO	Main Office
MUS	Monetary Unit Sampling
NAO	National Audit Office
NDPBs	Non-Departmental Public Bodies
NED	Non-Executive Director
NHS	National Health Service
NII	Nuclear Installations Inspectorate
NYSE	New York Stock Exchange
OC	Output Control
OECD	Organization for Economic Cooperation and Development
PA	Performance Appraisal
PAC	Public Accounts Committee
PAF	Public Audit Forum
PC	Processing Control
PC	Personal Computer
PC	Plans and Control
PESTL	Political, Economical, Social, Technical and Legal
PI	Performance Indicator
PIIA	Diploma in Internal Audit Practice
PIPEDA	Personal Information Protection and Electronic Documents Act
PM	Project Manager
PPF	Professional Practices Framework
PSR	Preliminary Survey Report
PwC	PricewaterhouseCoopers
QA	Quality Assurance
QRP	Quality Review Process
RaCE	Risk and Control Evaluation
RBSA	Risk-Based Systems Auditing
SBA	Systems-Based Auditing
SBA	Systems-Based Approach
SD	Systems Development
SD	Standard Deviation
SEC	Securities and Exchange Commission
SEC	Stock Exchange Commission
SEE	Social Ethical and Environmental
SIC	Statement on Internal Control
SIMEX	Singapore International Money Exchange
SLAs	Service Level Agreements
SWOT	Strengths, Weaknesses, Opportunities and Threats

TBA	Transactions Based Approach
TEC	Training & Enterprise Council
TI	Transparency International
TQM	Total Quality Management
UK	United Kingdom
USA	United States of America
VFM	Value for Money

FOREWORD TO SECOND EDITION

Internal auditing is a profession which has always prided itself on being a service to management. That service was founded on the ability of internal auditors to influence the way in which managers controlled their organization's operations in order to achieve objectives. Internal auditors have never attempted to take over the management task – rather they have tried to support the manager's endeavours by reviewing and advising in order to give an assurance that control is as effective as it can be.

The function of internal auditing can be undertaken in a variety of ways and it is for each organization to discover the best way for itself. In-house teams know the business; outsource providers and partnerships bring other strengths. Boards of directors must decide from all the options open to them which type of service is most likely to work for them, is the most cost-effective and adds the most value.

It is clear, however, that at the start of the third millennium, internal auditing has a significant role to play in every type of organization and in every economic centre. The late twentieth century saw virtually every type of organization suffer to some extent from poor management decisions, unethical corporate behaviour, fraud and other unacceptable business practices. Thus, corporate governance – *the way in which organizations are directed and controlled* – and a worldwide interest in the wider stakeholder community has meant that boards of directors have come under more scrutiny than ever before.

Accountability, transparency of operations and the integrity of boards and their individual members have resulted in global pressure on organizations to fully understand their corporate objectives and the impact, both socially and environmentally, which these objectives may have. Additionally, organizations must assess and manage the risks which may prevent attainment of objectives and convince their stakeholders that outputs of product or service have been achieved as economically, efficiently and effectively as is practicable.

All of this allows the internal auditor to move centre-stage. The skills in which internal auditors have always excelled – understanding strategic planning and objective setting; assessing and prioritizing risks; recommending control and mitigation strategies; communication ability – mean that more than ever before boards and senior managers are seeking the help of well-qualified, professional internal auditors to assist them in this increasingly complex technological world.

Internal auditors have not been slow to take up the challenge and this Handbook exemplifies the approach of continuous improvement which all professionals need in order to provide the service which managers need. Calling upon modern approaches and the use of technology to achieve greater productivity and understanding, the Handbook draws upon global best practice together with illustrations and examples from experienced practitioners. For both the new-entrant to internal auditing and the more experienced professional, Spencer Pickett has ensured that this updated version of the Handbook provides the material which will add to everyone's store of knowledge.

In times of fast change, technological innovation and pressure to deliver in virtually all sectors of activity, the Handbook provides the right guidance to achieve greater learning. More than this, it gives the stimulus for each of us to continue to improve our professional approach to providing an effective internal audit service.

Neil Cowan
Past President, IIA.UK&Ireland
IIA Global Ambassador

ACKNOWLEDGEMENTS

A very special thanks to my wife, Jennifer, for all her help and support in preparing the new edition and a big hug to our children Dexter and Laurel-Jade; just for being there.

For their past, present and continuing support, a thank you to Nigel Freeman, Neil Cowan, Richard Todd, Andy Wynne, Professor Andrew Chambers, Dan Swanson, Vernon Bailey, Paul Moxey, John Watts, Marian Lower, Eric Hall, Keith Wade, Graham Westwood, Steve Hardman, Mr and Mrs Livermore, Mr and Mrs Newman, Master Lajos Jakab, Mohammed Khan, Horace Edwards, Hock-Chye Ong, Don Daniels, Jack Stephens, Sue Seamour, Adrian Hogg, Mike Mintrum, Alan Davies, Tony Otokito, and staff at the Institute of Internal Auditors (UK&Ireland). Also a thank you to my large family including Aunt Edith, Aunt Joyce, Uncle Tony, and also: Tony, Graham, Kathy, Ellen, James, Lenny, Marianne (Maza), Lucie, Stella, Adrian, Maria, Irvine, Nigel, Nichole, Trevor, Barbara, Michael, Elaine and Karron.

A very special acknowledgement to Professor Gerald Vinten, Editor of the *Managerial Auditing Journal*, who introduced me to the previously mysterious world of the author.

Chapter 1

INTRODUCTION

Introduction

The third edition of the *Internal Auditing Handbook* reflects the significant changes in the field of internal auditing over the last few years. Since the last edition, there have been many developments that impact the very heart of the audit role. There really are 'new look' internal auditors who carry the weight of a heightened expectation from society on their shoulders. Auditors no longer spend their time looking down at detailed working schedules in cramped offices before preparing a comprehensive report on low-level problems that they have found for junior operational managers. They now spend much more time presenting 'big picture' assurances to top executives after having considered high-level risks that need to be managed properly. Moreover, the internal auditor also works with and alongside busy managers to help them understand the task of identifying and managing risks to their operations. At the same time, the internal auditor has to retain a degree of independence so as to ensure the all-important professional scepticism that is essential to the audit role. The auditor's report to the board via the Audit Committee must have a resilience and dependability that is unquestionable. These new themes have put the internal auditor at the forefront of business and public services as one cornerstone of corporate governance – and the new *Internal Auditing Handbook* has been updated to take this on board. The third edition of the *Internal Auditing Handbook* contains all the detailed material that formed the basis of the second edition and has been expanded in the following manner:

1. The new edition has been updated to reflect the Institute of Internal Auditor's (IIA) International Standards for the Professional Practice of Internal Auditing that were released during 2009.
2. Each chapter has a new section on new developments to reflect changes that have occurred since the second edition was published.
3. A series of multi-choice questions has been developed and included at the end of each chapter.
4. A number of important contributions from Dan Swanson on Information Systems auditing and other topics have been included throughout the book.

Change is now a constant and we have tried not to focus too much on specific events such as the 2007/2008 Credit Crunch, the resulting recession and the Madoff fraud, since it is the principles of internal auditing that remain constant, regardless of the latest scandal to impact the economy. Please have a look at the IIA's web site at www.theiia.org to keep up to date with latest developments.

Back in 1997, the first edition of the Handbook described internal auditing as a growing quasi-profession. The quantumleap that occurred between the old and the new millennium is that internal auditing has now achieved the important status of being a full-blown profession. Note that the term chief audit executive (CAE) is used throughout the handbook and this person is described by the IIA:

> The chief audit executive is a senior position within the organization responsible for internal audit activities. Normally, this would be the internal audit director. In the case where internal audit activities are obtained from external service providers, the chief audit executive is the person responsible for overseeing the service contract and the overall quality assurance of these activities, reporting to senior management and the board regarding internal audit activities, and follow-up of engagement results. The term also includes titles such as general auditor, head of internal audit, chief internal auditor, and inspector general.

The areas that are included in this chapter are:

1.1 Reasoning behind this Book
1.2 The IIA Standards and Links to the Book
1.3 How to Navigate around the Book
1.4 The Handbook as a Development Tool
1.5 The Development of Internal Auditing
Summary and Conclusions
Assignments and Multi-choice Questions

1.1 Reasoning behind the Book

The original *Internal Auditing Handbook* focused on the practical aspects of performing the audit task. It contained basic material on managing, planning, performing and reporting the audit, recognizing the underlying need to get the job done well. The new edition has a different focus. Now, we first and foremost need to understand the audit context and how we fit into the wider corporate agenda. It is only after having done this that we can go on to address the response to changing expectations. In fact, we could argue that we need to provide an appropriate response rather than think of the audit position as being fixed and straightforward. It is no longer possible to simply write about an audit programme and how this is the best way to perform the audit task. To do justice to the wealth of material on internal auditing, we must acknowledge the work of writers, thought leaders, academics, journalists and noted speakers at internal audit (IA) conferences. The first and second editions of the *Internal Auditing Handbook* set out the author's views and understanding of the audit role. The new Handbook contains a whole range of different views and extracts of writings from a variety of representatives from the audit community. There are also special contributions from Richard Todd and Andy Wynne who have provided several examples, written specially for the Handbook, taken from their many years of professional internal auditing work. Gerald Vinten, Paul Moxey, Mohammed Khan, John Watts and Neil Cowan have likewise shared their experiences with the reader. Dan Swanson has provided many important contributions to the new handbook. Dan is an IA veteran who is also a former director of professional practices at the IIA. He has completed audit projects for more than 30 different organizations and has almost 25 years of auditing experience in government at federal, provincial and municipal levels, as well as in the private sector. Dan Swanson has also been a long-time columnist for *Compliance Week*, a leading US governance, risk and compliance publication.

The new context for internal auditing is set firmly within the corporate governance arena. The IIA definition of internal auditing was not changed when the standards were revised in January 2009 and remains as follows:

> Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives

by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.

The *Internal Auditing Handbook* has early chapters on Corporate Governance Perspectives, Managing Risk and Internal Controls. It is only after having addressed these three inter-related topics that we can really appreciate the IA role. There are chapters on quality, professional standards, audit approaches, managing IA, planning, performance and reporting audit work and specialist areas such as fraud and IS auditing. The final chapter attempts to look at our future and changes that may well be on the way. The new Handbook includes several new references and quotes from a wide variety of sources; since all views are important, even where they conflict. This variety can only help move the profession onwards and upwards. The Handbook rests firmly on the platform provided by the International Standards for the Professional Practice of Internal Auditing as part of the International Professional Practices Framework (IPPF). Internal auditing is a specialist career and it is important that we note the efforts of a professional body that is dedicated to our chosen field. Note that despite the recent changes in the field of internal auditing, there is much of the first book that is retained in the new edition. Change means we build on what we, as internal auditors, have developed over the years rather than throw away anything that is more than a few years old. That is why the original material from the second edition has not been discarded, as the saying goes – it is important not to throw away the baby with the bath water. Note that all references to IIA definitions, code of ethics, IIA attribute and performance standards, practice advisories and practice guides relate to the IPPF prepared by the IIA in 2009.

1.2 The IIA Standards and Links to the Book

The Handbook addresses most aspects of internal auditing that are documented in the IIA International Standards for the Professional Practice of Internal Auditing. In late 2005, the IIA's Executive Committee commissioned an international Steering Committee and Task Force to review the Professional Practices Framework (PPF), the IIA's guidance structure and related processes. The Task Force's efforts were focused on reviewing the scope of the framework and increasing the transparency and flexibility of the guidance's development, review and issuance processes. The results culminated in a new IPPF and a reengineered Professional Practices Council, the body that supports the IPPF. The Attribute Standards outline what a good IA setup should look like, while the Performance Standards set a benchmark for the audit task. Together with the Practice Advisories, Position Statements and Practice Guides and other reference material (as at October 2009), they constitute a professional framework for internal auditing. The IIA's main Attribute and Performance Standards are listed below:

ATTRIBUTE STANDARDS

1000 – Purpose, Authority, and Responsibility
The purpose, authority, and responsibility of the internal audit activity must be formally defined in an internal audit charter, consistent with the Definition of Internal Auditing, the Code of Ethics, and the Standards. The chief audit executive must periodically review the internal audit charter and present it to senior management and the board for approval.

1100 – Independence and Objectivity
The internal audit activity must be independent, and internal auditors must be objective in performing their work.

1200 – Proficiency and Due Professional Care
Engagements must be performed with proficiency and due professional care.

1300 – Quality Assurance and Improvement Program
The chief audit executive must develop and maintain a quality assurance and improvement program that covers all aspects of the internal audit activity.

PERFORMANCE STANDARDS

2000 – Managing the Internal Audit Activity
The chief audit executive must effectively manage the internal audit activity to ensure it adds value to the organization.

2100 – Nature of Work
The internal audit activity must evaluate and contribute to the improvement of governance, risk management and control processes using a systematic and disciplined approach.

2200 – Engagement Planning
Internal auditors must develop and document a plan for each engagement, including the engagement's objectives, scope, timing and resource allocations.

2300 – Performing the Engagement
Internal auditors must identify, analyze, evaluate, and document sufficient information to achieve the engagement's objectives.

2400 – Communicating Results
Internal auditors must communicate the engagement results.

2500 – Monitoring Progress
The chief audit executive must establish and maintain a system to monitor the disposition of results communicated to management.

2600 – Resolution of Senior Management's Acceptance of Risks
When the chief audit executive believes that senior management has accepted a level of residual risk that may be unacceptable to the organization, the chief audit executive must discuss the matter with senior management. If the decision regarding residual risk is not resolved, the chief audit executive must report the matter to the board for resolution.

1.3 How to Navigate around the Book

A brief synopsis of the Handbook should help the reader work through the material. It is clear that the Handbook is not really designed to be read from front to back but used more as a reference resource. Having said that, there should be some logic in the ordering of the material so that it fits together if the reader wishes to work through each chapter in order. One important point to make is that although most chapters contain 10 main sections, they are each of variable length. Some readers find different chapter lengths inconvenient, but there is little point trying to fit set material into standard boxes when some chapters naturally consume more material than others. In fact, some sections are quite long because they need to cover so much ground. Apologies in advance if this policy proves bothersome at all.

Chapter 1 – Introduction

This first chapter deals with the content of the handbook and lists the International Standards for the Professional Practice of Internal Auditing. It also covers the way the handbook can be used as

a development tool for the IA staff, linked to website material that can be used to form the basis of learning workshops and resources. The way internal auditing has developed over the years is an important aspect of the chapter, whereby the progress of the profession is tracked in summary form from its roots to date. It is important to establish the role of IA at the start of the book to retain this focus throughout the next few chapters that cover corporate perspectives. Note that the IA process appears in some detail from Chapter 5 onwards. Likewise our first encounter with the IPPF appears in this chapter based on the 'Platform' theory to underpin the entire Handbook.

Chapter 2 – Corporate Governance Perspectives

Chapter 2 covers corporate governance in general, in that it summarizes the topic from a business standpoint rather than focusing just on the IA provisions. A main driver for 'getting things right' is the constant series of scandals that have appeared in every developed (as well as developing) economy. The governance equation is quickly established, and then profiles of some of the well-known scandals are used to demonstrate how fragile the accountability frameworks are. New look models of corporate governance are detailed using extracts from various codes and guidance to form a challenge to business, government and not-for-profit sectors. Note that the chapter may be used by anyone interested in corporate governance as an introduction to the subject. The section on internal auditing is very brief and simply sets out the formal role and responsibilities, without going into too much detail. One topic that stands out in the chapter relates to audit committees as many view this forum as the key to ensuring corporate responsibility and transparency. The corporate governance debate is ongoing and each new code refers to the need to start work on updates almost as soon as they are published. As such, it is never really possible to be up to date at publication and the reader is advised to keep an eye on new developments as and when they arise.

Chapter 3 – Managing Risk

Many writers argue that we are entering a new dimension of business, accounting and audit whereby risk-based strategies are essential to the continuing success of all organizations. Reference is made to various risk standards and policies, and we comment on the need to formulate a risk management cycle as part of the response to threats and opportunities. The corporate aspiration to embed risk management into the way an organization works is touched on. The growing importance of control self-assessment has ensured this appears in the Handbook, although this topic is also featured in the chapter on audit approaches. The chapter closes with an attempt to work through the audit role in risk management and turns to the published professional guidance to help clarify respective positions. There is a link from this chapter to risk-based planning in the later chapter on Setting an Audit Strategy. Throughout the Handbook, we try to maintain a link between corporate governance, risk management and internal control as integrated concepts.

Chapter 4 – Internal Controls

Some noted writers argue that internal control is a most important concept for internal auditors to get to grips with. Others simply suggest that we need to understand where controls fit into the risk management equation. Whatever the case, it is important to address this topic before we can get into the detailed material on internal auditing. An auditor armed with a good control

model is more convincing that one who sees controls only as isolated mechanisms. Chapter 4 takes the reader through the entire spectrum of control concepts from reasoning, control models, procedures, and the link to risk management. One key section concerns the fallacy of perfection where gaps in control and the reality of imperfection are discussed. This forms the basis for most business ventures where uncertainty is what creates business opportunities and projects. With the advent of risk management, this does not mean controls take a back seat; it just means controls need to add value to the business equation.

Chapter 5 – The Internal Audit Role

This chapter moves into the front line of IA material. Having got through the reasoning behind the audit role (governance, risk management and control), we can turn to the actual role. The basic building blocks of the charter, independence, ethics and so on are all essential aspects of the Handbook. Much of the material builds on the original first edition of the Handbook and is updated to reflect new dimensions of auditing. One key component is the section on audit competencies, which forms the balancing factor in the equation – 'the challenges' and 'meeting the challenges'. Most auditors agree that there is the set audit role and then there are variations of this role. Those who have assumed one particular variation of the audit role need to appreciate where it fits into the whole.

Chapter 6 – Professionalism

The auditors' work will be determined by the needs of the organization and the experiences of senior auditors, and most audit shops arrive at a workable compromise. One feature of the upwards direction of the IA function is the growing importance of professional standards as a third component of the equation we discussed earlier. Some of the published standards are summarized in this chapter, although the main footing for the Handbook revolves around the IPPF. Moreover, quality is a theme that has run across business for many years. If there are quality systems in place, we are better able to manage the risk of poor performance. It would be ironic for IA reports to recommend better controls over operations that are reviewed when the audit team has no system in place that ensures it can live up to professional standards. Processes that seek to improve the IA product are covered in this chapter, including the important internal and external reviews that are suggested by audit standards.

Chapter 7 – The Audit Approach

The range and variety of audit services that fall under the guise of internal auditing have already been mentioned. A lot depends on the adopted approach and rather than simply fall into one approach, it is much better to assess the possible positions armed with a knowledge of what is out there. Once we know what we will be providing, we can think about a suitable structure for the audit shop. The growing trend to outsourcing the IA function has meant a separate section on this topic with an illustration. Control risk self-assessment (CRSA) is also detailed along with tips on facilitation skills. It is possible to integrate the CRSA technique with the audit process and this interesting concept is the feature of this chapter. Other specialist audit work involving management investigations, fraud investigations and information systems auditing is also mentioned. The IPPF acknowledge the linked trend towards more consulting work by IA outfits and the consulting approach has its own section.

Chapter 8 – Setting an Audit Strategy

One view is that formulating an IA strategy is one of the most important tasks for the CAEs. In itself, this task depends on an intimate understanding of the corporate context, the audit role and competencies and challenges that add value to the business. The CAE needs to define a strategy, set standards, motivate staff and then measure what is done to have a half chance at delivering a successful audit service. The chapter includes a section on establishing a new audit shop, by bringing everything together, either in-house or through outsourced arrangements.

Chapter 9 – Audit Field Work

Audit field work covers the entire audit processes from planning the assignment to reporting the results, while interviewing is the primary means of obtaining information for the audit. One interesting aspect of this chapter is the section on working papers. This section on working papers establishes that good working papers can help develop findings and the draft report. Formal presentations are becoming increasingly popular and this is dealt with in this chapter.

Chapter 10 – Meeting the Challenge

This final short chapter attempts to track key developments that impact on internal auditing and includes comments from various sources on its future direction.

1.4 The Handbook as a Development Tool

All internal auditors need to be professionally competent and all IA shops need likewise to demonstrate that they add value to the risk management, control and governance processes. While a great deal of high-level work may be undertaken by the CAE in terms of strategy, budgets and audit plans, the bottom line comes down to the performance of each and every individual auditor. It is this person who must carry the burden of the expectation that IA will be a foundation for governance in the employing organization. The *Internal Auditing Handbook* is a collection of reference material that can be used to help support the internal auditor's constant drive to professionalism. It contains a basic foundation of audit information that should be assimilated by competent internal auditors. The handbook can also be used as an induction tool for new auditors where they work through each chapter and then under the supervision of an appointed coach are encouraged to tackle the relevant assignments and multi-choice questions at the end of most chapters. In this way, new staff members can be monitored as they submit their written response to each set of questions. It should take around two weeks to work through the handbook and prepare formal responses to each chapter's set questions (see Appendix A).

1.5 The Development of Internal Auditing

IA is now a fully developed profession. An individual employed in IA 10 years ago would find an unrecognizable situation in terms of the audit role, services provided and approach. For a full appreciation of internal auditing, it is necessary to trace these developments and extend trends into the future. It is a good idea to start with the late Lawrence Sawyer, known as the Godfather

of IA, to open the debate on the audit role. Sawyer has said that audit has a long and noble history: 'Ancient Rome "hearing of accounts" one official compares records with another – oral verification gave rise to the term "audit" from the Latin "auditus" – a hearing'.[1]

The Evolution of the Audit Function

It is important to understand the roots of internal auditing and the way it has developed over the years. One American text has detailed the history of IA:

> Prior to 1941, internal auditing was essentially a clerical function . . . Because much of the record keeping at that time was performed manually, auditors were needed to check the accounting records after it was completed in order to locate errors . . . railroad companies are usually credited with being the first modern employers of internal auditors . . . and their duty was to visit the railroads' ticket agents and determine that all monies were properly accounted for. The old concept of internal auditing can be compared to a form of insurance; the major objective was to discover fraud . . . .[2]

It is clear that the IA function has moved through a number of stages in its development.

Extension of external audit IA developed as an extension of the external audit role in testing the reliability of accounting records that contribute to published financial statements. IA was based on a detailed programme of testing of accounting data. Where this model predominates, there can be little real development in the professionalism of the IA function. It would be possible to disband IA by simply increasing the level of testing in the external auditor's plans. Unfortunately, there are still organizations whose main justification for resourcing an IA service is to reduce the external audit fee. The Institute of Internal Auditors in the United Kingdom and Ireland (IIA.UK&Ireland) have suggested this link between external and IA:

> The nineteenth century saw the proliferation of owners who delegated the day-to-day management of their businesses to others. These owners needed an independent assessment of the performance of their organizations. They were at greater risk of error, omissions or fraud in the business activities and in the reporting of the performance of these businesses than owner-managers. This first gave rise to the profession of external auditing. External auditors examine the accounting data and give owners an opinion on the accuracy and reliability of this data. More slowly the need for internal auditing of business activities was recognized. Initially this activity focused on the accounting records. Gradually it has evolved as an assurance and consulting activity focused on risk management, control and governance processes. Both external audit and internal audit exist because owners cannot directly satisfy themselves on the performance and reporting of their business and their managers cannot give an independent view of these.[3]

Internal check The testing role progressed to cover non-financial areas, and this equated the IA function to a form of internal check. A large number of transactions were double-checked to provide assurances that they were correct and properly authorized by laid-down procedures. The infamous 'audit stamp' reigned supreme indicating that a document was deemed correct and above board. Internal control was seen as internal check and management was presented with audit reports listing the sometimes large number of errors found by IA. The audit function usually consisted of a small team of auditors working under an assistant chief accountant. This

actually encouraged management to neglect control systems on the grounds that errors would be picked up by auditors on the next visit. It locked the audit role tightly into the system of control, making it difficult to secure real independence. If existence within an organization depends on fulfilling a service need, then this need must be retained if it is to survive. The temptation is to encourage failings in the systems of control so that each visit by the internal auditor could result in a respectable number of audit findings. Wide-ranging recommendations for solving these control gaps (which cause these errors in the first place) may, therefore, not be made by the auditor.

Probity work Probity work arrived next as an adaptation of checking accounting records where the auditors would arrive unannounced at various locations and local offices, and perform a detailed series of tests according to a preconceived audit programme. Management was presented with a list of errors and queries that were uncovered by the auditors. The auditors either worked as a small team based in accountancy or had dual posts where they had special audit duties in addition to their general accounting role. Audit consisted mainly of checking, with the probity visits tending to centre on cash income, stocks, purchases, petty cash, stamps, revenue contracts and other minor accounting functions. The main purpose behind these visits was linked to the view that the chief accountant needed to check on all remote sites to ensure that accounting procedures were complied with and that their books were correct. The audit was seen as an inspection on behalf of management. This militates against good controls, as the auditor is expected to be the main avenue for securing information. Insecure management may then feel that their responsibility stops at issuing a batch of detailed procedures to local offices and nothing more. The auditors would then follow up these procedures without questioning why they were not working. The fundamental components of the control systems above local-office level fell outside the scope of audit work that was centred on low-level, detailed checking.

Non-financial systems The shift in low-level checking arose when audit acquired a degree of separation from the accounting function with IA sections being purposely established. This allowed a level of audit management to develop, which in turn raised the status of the audit function away from a complement of junior staff completing standardized audit programmes. The ability to define an audit's terms of reference stimulated the move towards greater professionalism, giving rise to the model of audit as a separate entity. Likewise, the ability to stand outside basic financial procedures allowed freedom to tackle more significant problems. It was now possible to widen the scope of audit work and bring to bear a whole variety of disciplines including civil engineering, statistics, management, computing and quality assurance.

Chief auditors Another thrust towards a high-profile, professional audit department was provided through employing chief internal auditors (or CAEs) with high organizational status. They could meet with all levels of senior management and represent the audit function. This tended to coincide with the removal of audit from the finance function. The audit department as a separate high-profile entity encourages career auditors, able to develop within the function. This is as well as employing people who are able to use this audit experience as part of their managerial career development. The current position in many large organizations establishes a firm framework from which the audit function may continue to develop the professional status that is the mark of an accepted discipline. When assessing risk for the audit plan, one asks what is crucial to the organization before embarking on a series of planned audits that in the past may have had little relevance to top management. Professionalism is embodied in the ability to deal with important issues that have a major impact on success. The recent rise in the profile of internal auditing confirms this potential for significant development.

Audit committees Audit committees bring about the concept of the audit function reporting to the highest levels and this had a positive impact on perceived status. Securing the attention of the board, chief executive, managing director, non-executive directors and senior management also provides an avenue for high-level audit work able to tackle the most sensitive corporate issues. This is far removed from the early role of checking the stock and petty cash. IA was now poised to enter all key parts of an organization. An important development in the US occurred when the Treadway Commission argued that listed companies should have an audit committee composed of non-executive directors. Since then, most stock exchange rules around the world require listed companies to have an audit committee.

Professionalism The IIA has some history going back over 50 years. *Brink's Modern Internal Auditing* has outlined the development of the IIA:

> In 1942, IIA was launched. Its first membership was started in New York City, with Chicago soon to follow. The IIA was formed by people who were given the title internal auditor by their organizations and wanted to both share experiences and gain knowledge with others in this new professional field. A profession was born that has undergone many changes over subsequent years.[4]

The Development of Internal Audit Services

The developmental process outlined above highlights the way the function has progressed in assuming a higher profile and a greater degree of professionalism. The type of audit service has changed to reflect these new expectations and these developments over the last 20 years may likewise be traced:

1. Internal check procedures IA was seen as an integral component of the internal checking procedures designed to double-check accounting transactions. The idea was to re-check as many items as possible so as to provide this continuous audit. One might imagine an audit manager giving staff an instruction that 'your job is to check all the book entries' on an ongoing basis.

2. Transaction-based approach The transactions approach came next, where a continuous programme of tests was used to isolate errors or frauds. This checking function became streamlined so that a detailed programme of tests was built up over time to be applied at each audit visit. This systematic approach is readily controlled so that one might have expected the auditor to complete hundreds of checks over a week-long period during the course of completing this predetermined audit programme.

3. Statistical sampling Statistical sampling was later applied to reduce the level of testing along with a move away from examining all available documents or book entries. A scientific approach was used, whereby the results from a sample could be extrapolated to the entire population in a defendable manner. The problem is that one is still adopting the external audit stance that seeks to give an accept or reject decision as the final product. Like the sophisticated computer interrogation now used in audit work, this is an example of how a new technique is limited by a refusal to move away from traditional audit objectives. The downfall of many an information system's auditor has been failure to understand the full impact of the audit role. Computerized investigations now allow 100% checks, although much depends on whether we perceive this as a valid audit task or a managerial responsibility.

4. Probity-based work Probity-based work developed next, again featuring the transaction approach where anything untoward was investigated. The probity approach is based on audit being the unseen force that sees and hears all that goes on in the organization. Instead of double-checking accounting records and indicating those that should be corrected, the probity approach allowed the chief accountant to check on financial propriety across the organization. The auditor would represent the director of finance (DF) by visiting all major units and carrying out these audit test programmes.

5. Spot checks It was then possible to reduce the level of probity visits by making unannounced spot checks so that the audit deterrent (the possibility of being audited) would reduce the risk of irregularity. Larger organizations may have hundreds of decentralized locations that would have been visited each year by the auditor. This service depends on employing large teams of junior auditors who would undertake these regular visits. As management started to assume more responsibility for its operations, the audit service turned increasingly to selective as opposed to periodic visits. Rather than a guaranteed visit each year, one sought compliance with procedure by threatening the possibility of a visit. It has been suggested that: 'combining the need for uncovering errors and the need to catch misappropriations resulted in the internal auditor being little more than a verifier.'[5]

Moreover, most internal auditors assumed a 'Got-Ya' mentality where their greatest achievements resided in the task of finding errors, abuse and/or neglect by managers and their staff. One writer has said: 'The old concept of internal auditing can be compared to a form of insurance; the major objective was to discover fraud more quickly than it could be discovered by the public accountant during an annual audit.'[6]

6. Risk analysis The transaction/probity approach could be restricted by applying a form of risk analysis to the defined audit areas so that only high risk ones would be visited. There are many well-known risk formulae that are designed to target audit resources to specific areas based around relevant factors. Each unit might then be ranked so that the high risk ones would be visited first and/or using greater resources. Risk analysis used in conjunction with statistical sampling and automated interrogation gives the impression that internal auditing is carried out wholly scientifically, although this approach is steeped in the dated version of internal auditing.

7. Systems-based approach Then came a move away from the regime of management by fear to a more helpful service. Systems-based audits (SBAs) are used to advise management on the types of controls they should be using. Testing is directed more at the controls than to highlight errors for their own sake. The problems found during audit visits will ultimately be linked to the way management controls its activities. This new-found responsibility moves managers away from relying on the programmed audit visit to solve all ills. Systems of control become the keywords that management adopts when seeking efficiency and effectiveness, and formed the focus of the audit service. The application of SBA was originally directed at accounting systems where internal control questionnaires devised by external auditors were adapted and used. Basic financial systems were covered by tailoring ready-made audit programmes that looked for a series of predetermined controls. These were applied by internal auditors, although it was still in the shadow of external audit work. The importance of sound organizational systems came to the fore in the US where the Foreign Corrupt Practices Act passed in 1997 stated that an organization's management was culpable for any illegal payments made by the organization even where they claimed they had no knowledge of the payments. The only way to ensure legality and propriety of all payments was to install reliable systems and controls.

8. Operational audit Attention to operational areas outside the financial arena provided an opportunity to perform work not done by the external auditor. The concepts of economy, efficiency and effectiveness were built into models that evaluated the value-for-money (VFM) implications of an area under review. Looking for savings based on greater efficiencies became a clear part of the audit role. Purpose-built VFM teams were set up to seek out all identifiable savings. The worst-case scenario came true in many organizations where these teams had to be resourced from the savings they identified. It is one thing to recommend a whole series of savings but another to actually achieve them. As a result, many teams were later disbanded. On the other hand, operational audit teams that encouraged management to look for its own VFM savings had more success and this is now an established audit role.

9. Management audit Management audit moves up a level to address control issues arising from managing an activity. It involves an appreciation of the finer points relating to the various managerial processes that move the organization towards its objectives. This comes closer to the final goal of IA where it is deemed capable of reviewing all-important areas within the organization by adopting a wide interpretation of systems of control. The ability to understand and evaluate complicated systems of managerial and operational controls allows audit to assume wide scope. This is relevant where controls are seen in a wider context as all those measures necessary to ensure that objectives are achieved. The systems-based approach offers great potential with the flexibility in applying this approach to a multitude of activities and developing a clear audit methodology at corporate, managerial and operational levels.

The late Gerald Vinten has argued that social auditing is the highest plane that IA may reach and defines this as: 'A review to ensure that an organisation gives due regard to its wider social responsibilities to those both directly and indirectly affected by its decisions and that a balance is achieved between those aspects and the more traditional business or service-related objectives.'[7]

10. Risk-based auditing Many IA shops have now moved into risk-based auditing where the audit service is driven by the way the organization perceives and manages risk. Rather than start with set controls and whether they are being applied throughout the organization properly, the audit process starts with understanding the risks that need to be addressed by these systems of internal control. Much of the control solution hinges on the control environment in place and whether a suitable control framework has been developed and adopted by the organization. IA can provide formal assurances regarding these controls. Moreover, many IA shops have also adopted a consulting role, where advice and support are provided to management.

This is no linear progression in audit services with many forces working to take the profession back to more traditional models of the audit role where compliance and fraud work (financial propriety) are the key services in demand.

Moving Internal Audit out of Accountancy

Many of the trends behind the development of IA point to the ultimate position where the audit function becomes a high-profile autonomous department reporting at the highest level. This may depend on moving out audit functions currently based in accountancy. It is possible to establish IA as a separate profession so that one would employ internal auditors as opposed to accountants. This is a moot point in that there are those who feel that the auditor is above all an accountant. Not only is this view short-sighted but it is also steeped in the old version of the internal auditor as a poor cousin of the external auditor. The true audit professional is called upon

to review complicated and varied systems even if the more complicated and sensitive ones may sometimes be financially based. A multidisciplined approach provides the flexibility required to deal with operational areas. Many organizations require internal auditors to hold an accounting qualification or have accountancy experience. A move outside the finance function allows staff to be employed without an accounting background. There are clear benefits in this move in terms of securing a firmer level of independence from the finance function:

- The traditional reporting line to the DF may have in the past created a potential barrier to audit objectivity. It may be said that there is little real audit independence where the CAE works for the DF. There are many models of internal auditing that see this function as a compliance role, representing the DF's interest in financial propriety. The auditor is able to comment on non-compliance so long as it does not extend to criticizing the DF. The corporate view of financial management relies on the DF taking responsibility for establishing sound financial systems, which are then devolved across an organization. The heart of any financial system will be based in the DF's department and this creates a problem for an auditor who may have found inadequacies in the way the DF has managed these systems. A defensive DF may ensure that the auditor does not produce material that forms a criticism of his/her financial services. This impairs the basic concept of independence where the auditor may be gagged, notwithstanding the presence of an audit committee.
- One might, therefore, give greater attention to the managerial aspects of providing financial systems and move away from merely checking the resulting transactions. This is one sure way of extending the potential scope of IA to enable it to tackle the most high-level, sensitive areas. The audit terms of reference will move beyond fraud and accounting errors to take on board all-important issues that impact on organizational controls. We are not only concerned with the matters affecting the DF but also that which is uppermost in the minds of the corporate management team headed by the chief executive. At this extreme, it becomes possible to audit the whole direction of the organization in terms of its corporate strategy that is a far cry from checking the petty cash and stocks.
- The relationship with external audit may become better defined where the differing objectives are clarified. The temptation for the DF to treat IA as an additional resource for external audit may decline. It may be possible to encourage external auditors to cover the main financial systems, with IA turning its attention more towards operational matters. If IA assumes a high profile and reviews the major activities, then the relationship between IA and external audit may be reversed. External audit may be seen to feed into the all-important IA process.
- The audit approach may move from an emphasis on financial audits to the exciting prospect of reviewing the entire risk management process itself. This change in emphasis is important; it is based on viewing the principal controls in any system of internal control as embodied in management itself. We would not consider the personalities of individual managers. We are more concerned with the formal managerial processes that have been established and how well they contribute to the efficient and effective application of resources. This allows the scope of internal auditing to move to almost unlimited horizons.
- The potential for establishing a powerful CAE may arise, which might be compared to the previous position where the CAE merely acted as a go-between for the DF and the audit staff, giving them batches of projects that the DF wanted done. In an ideal world, the CAE will have the ear of the chief executive officer (CEO) who may turn to audit for advice on major organizational issues that impact on underlying control systems. This has a knock-on effect with the CAE assuming a senior grade commensurate with his/her role in the organization. Likewise, audit managers and other staff will benefit. The IA department could end up with higher grades than the accountancy department.

In short, we would need to be close to, but at the same time be some distance from, the DF. However, as we move into the era of the audit committee, and the stronger links with this forum and IA, things are changing. The trend is for more of a break between the finance link as IA gets more and more involved in the actual business side of the organization. Again, this move is strengthened by the growing involvement in enterprise-wide risk management. The latest position is that there is normally no longer a clear logic to the CAE to continue to hold a reporting line to the DF. The debate now revoles around whether the CAE should report directly into the main board and not just to the audit committee.

The Role of the Statement of Responsibility

The IIA has issued various statements of responsibilities (SORs), each new one providing a revision to the previous. It is possible to trace much of the development of IA through these SORs from 1947 onwards:

1947 Original SOR setting out the first formal definition of IA. This saw the perceived role of IA as dealing primarily with accounting matters and is in line with the view that it arose as an extension of the external audit function.

1957 IA dealt with both accounting and other operations. Although the accounting function was the principal concern, non-accounting matters were also within the audit remit.

1971 The breakthrough came in viewing the audit field as consisting simply of operations. Accounting operations have to compete with all others for audit attention with no automatic right to priority.

1976 This is the same as in 1971 but is made gender-neutral so as not to assume that all auditors are male.

1981 The major change in this SOR is the alteration of defining IA from a service to management to a service to the organization. It directs the audit function to the highest levels of management. This impacts on independence in that the welfare of the organization becomes paramount as opposed to the requirements of individual managers. The new role of IA meant more attention to corporate areas with such a high-profile audit function.

1991 This SOR provides for greater flexibility to include a wider range of audit and consultancy services. This is balanced by raising the profile of the all-important concept of independence that is so difficult to achieve fully in practice. Issues of compliance with standards and ethics are more actively addressed, which must be accompanied by a firmer stance on member discipline that appears to be the trend with the IIA. Some of the more restrictive elements have been removed, which again allows a wider view of the audit role. To summarize, the statement recognizes that we may move further into consultancy but have to retain both professional standards and sufficient independence.

1994 The next definition appeared in the IIA standards in 1994 and includes the concept of ensuring that recommendations are made having due regard to the costs of implementing them. We may go further and suggest that all recommendations should incorporate a consideration of balancing costs with benefits before they may be applied. Interestingly, a return to a previous view can represent development. Basic audit concepts need not be thrown away with time.

1999 definition

> Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.

This brings the IA profession right up to date in being at the forefront of the corporate governance agenda and clarifies the dual aspects of the assurance and consulting roles that the new look IA function tends to entail. Note that the revised IPPF released in 2009 has not changed this formal definition of internal auditing.

The 1940s Debate

When the original SOR was being devised in the 1940s, it involved a debate as to the precise role and scope of internal auditing. Issues to be resolved before a clear model of audit could be constructed included:

1. Part of the system Is IA part of the system of internal control in terms of consisting mainly of checking the output from each main system before certifying that it is acceptable? This was certainly true in a number of IA departments where, for example, the 'audit stamp' meant that large payments were vetted before release and the auditor had other duties such as controlling important stationery. It was generally felt that this type of role was inappropriate and that IA should not be part of the routine systems-control procedures. We have certainly reached the point where audit cannot be locked into the systems of control as this may impair independence.

2. Reporting lines Who should IA report to? Here IA was seen primarily as part of the accounting function. One of the drawbacks is the continuing view that IA is mainly responsible for checking the accuracy of financial data. This would be in addition to its duties as a supreme force checking on operational management and its staff. The ability to audit the accounting function would be severely restricted by this position. IA being outside the accounting function continues to be a lively debate to this day. Most auditors accept that some remaining IA functions, particularly those established by legislation, are based in the finance department and that this does not necessarily mean a sufficiently independent service cannot be provided. Audit committees have now become popular and this may be seen as the ultimate client for audit services.

3. Control over controls Should IA be a control over internal controls? The response stresses the need for IA to be outside the system of internal control, although in this case a clearer link is defined. This is that audit reviews and evaluates the systems of control while not being an integrated component within the actual control routines. The definition of IA as a control over controls is clearly open to debate. Does this mean that the controls can operate without this floating control over them? Alternatively, does this floating audit control simply apply to areas planned for audit review via an appraisal of the relative risks of each unit? The definition of IA in the 1991 SOR suggested the definition was dated, although this comes back in the 1994 definition. The 2009 view of internal auditing reinforces the dual assurance and consulting roles in the context of risk management, control and governance processes.

4. External audit Co-ordination with external audit is accepted and all IA standards include this. The change that is now apparent is that IA should be an equal partner as opposed to an extension of external audit, and this depends on establishing a professional base. IA has much to offer an organization where a wider scope of its activities has been agreed and documented in an audit charter. There is still imbalance in the internal/external audit relationship apparent in organizations where, by convention, the external auditor reviews the IA function. The type of relationship that is assumed will depend on the personal strengths of the CAE. It should be based on the extent to which IA has adopted professional auditing standards. Sawyer has noted the difference between the two functions:

> The primary responsibility of the external auditor is to report on the organisation 's financial statements . . . internal auditors have a different function. It is broader and deeper than that of the external auditors. It furnishes managers throughout the organisation with information needed to effectively discharge their responsibilities.[8]

5. Management's role IA should not relieve management of its responsibilities. Management designs, implements and maintains effective systems of internal controls while audit's role is to review these systems and advise on those high-priority risk areas where control weaknesses need to be redressed by management. A systems approach would tend to be the most efficient way of achieving this. This is in contrast to a continual search for delinquent transactions that are generated by poor systems. This latter approach might imply that management need not secure good control since audit will catch all material errors. Unfortunately, this important principle is less easy to achieve in practice due to the political pressures found in all organizations. The temptation to prop up management and make oneself indispensable is far too evident for poorly conceived audit services. Being around at all times to bail senior managers out where they have not bothered to install proper systems of control may enhance the status of the audit function in the short term. By perpetuating this failure to secure good control, the long-term objective of the audit role in terms of improving controls will not be achieved and this will eventually be exposed.

6. Audit theory The debate continues as to whether IA should be based on pure theory or what is actually going on in practice. Imposing excessively high standards may create problems by excluding a proportion of the audit departments that are unable to meet these demanding requirements. Flexibility and professional standards are concepts that have to be reconciled so that suitable ideals may be defined but at the same time are attainable in practice. One must be wary of taking this concept of flexibility to the extreme since it may suggest that anyone can do an audit and there are in reality no clear standards to be observed. Theory must have some bearing on reality and if it is too far removed, then it may need to be adjusted through clear reasoning based on sound research. What is unacceptable is for audit practitioners to be ignorant of the range of audit theory and adopt suspect practices based on this lack of knowledge. This is quite different from assessing the current theory and, based on local factors, deciding to adopt a different, less demanding approach. The need to master the agreed common body of knowledge is fundamental to the advancement of internal auditing as a profession. It would appear, however, that we will need to establish just which services are covered by the IA umbrella and whether we adopt an open-door or more restrictive policy. This is linked to the wider question of whether we accept that IA is becoming progressively fragmented as a discipline, or whether we seek to exclude linked functions such as operational review, compliance, quality reviewers, inspectorates, and systems security. One solution would be to create a licensed IA practitioner. This individual would have to be a qualified member of the IA profession as a prerequisite to practising. This

would be particularly relevant where IA's presence is mandatory, since the requirement could be built into legislation and relevant codes of practice.

Influences on the Internal Audit Role

1. Contracting out internal audit All internal auditing departments are under threat. In the private sector, where IA is generally not mandatory, the in-house unit may be deleted, downsized or replaced by an inspectorate, quality assurance or operational review service. This is equally so in financial services where the compliance role may not necessarily be carried out by IA. The public sector is in the front line, facing external competition like an army preparing for war. Outsourcing in central and local government provides an avenue for public sector internal auditing to be undertaken by firms of accountants. This cannot be said to be targeting IA since it represents overall governmental policy with universal application across many countries of varying political persuasion. All CAEs should have a number of key issues uppermost in their minds including:

- A formal strategy for meeting competition from internal and/or external sources.
- The audit budget and current charge-out rates for each auditor and how these figures compare to other departments.
- The pricing strategy will fall between the ranges shown in Figure 1.1.



FIGURE 1.1 Audit pricing strategy.

The pricing strategy cannot be completed until marketing research has been carried out that establishes exactly what the client wants. This marketing exercise should be commissioned by the CAE and incorporated into the formal strategy. The level of resources should be assessed and compared to the current staff complement. Changes should be made over time so staff can be retired, made redundant, recruited and developed until a best possible position is achieved. The whole concept of quality audit procedures and methodologies will need to be subject to constant review. We can take a short cut in explaining what this entails by simply stating that all material matters would be covered if the audit manual is reviewed and updated as a priority. If the CAE is not concerned with the above matters, then the future welfare of the internal auditing function is left to chance, like a rudderless ship. These matters should, therefore, represent the most pressing concerns for the CAE over and above the day-to-day workload.

2. Globalization The big picture of internal auditing must include that it is a discipline universally applicable throughout the world. There is no formal requirement that all CAEs be qualified apart from organizational job specifications. There is, no worldwide concept of an internal auditor able to practise in any country. There is, however, a move to spread professional auditing practice from the developed world to the less developed. The IIA is the only body established solely for the promotion of internal auditing. The IIA's International Standards for the Professional Practice of Internal Auditing are applied in each member country with slight changes in terminology to accommodate local requirements, and there now exists a Global IIA with relevant representation from across the world.

3. Quality management The continuing interest in total quality management (TQM) is derived from a desire to secure excellence in service/product delivery. This allows a top downwards review of existing practices. Internal auditors are well versed in the principles and practice of management, which is examined in IIA examinations.

4. The compliance role There is some debate on the role of IA in compliance with procedure. The technical view argues we have moved away from detailed checking as the profession developed. One may now audit corporate systems of importance to the entire welfare of the organization. However, there are organizations such as banks and retail companies that make great play of compliance checks and have a need for an audit service that management knows and understands. Aspirations to professionalism may have to take second place to getting permanent business and guaranteeing one's future welfare. The picture is not as grey as might appear at first sight. There are many new compliance roles linked into major issues such as quality assurance, financial regulations, contract tendering and computer security that raise the profile of IA. One approach is to perform these services as an add-on to the main systems role.

5. Independence Much has been written on independence and it is no longer treated as an esoteric entity that is either held on to or given up through greed or ignorance. A response to the threat of external competition from the big accountancy firms was that they could not be independent. This argument is insufficient. Independence is perceived more practically as the basic ability to do a good job. It is, therefore, possible to offer consultancy services in addition to traditional audits, recognizing this new-found realism. How far this concept can be extended is a matter for informed judgement and debate.

6. The expectation gap Audit services will have to be properly marketed, which is essentially based on defining and meeting client needs. This feature poses no problem as long as clients know what to expect from their internal auditors. It does, however, become a concern when this is not the case, and there is a clear gap in what is expected and what is provided. Management may want internal auditors to:

- check on junior staff on a regular basis
- investigate fraud and irregularity and present cases to the police and/or internal disciplinaries
- draft procedures where these are lacking
- draft information papers on items of new legislation or practice
- investigate allegations concerning internal disputes and advise on best resolution
- advise on data protection and security, and check that the rules are complied with.

One cannot give up professional integrity but, at the same time, the above matters cannot be ignored. If new resources are brought in to cover these services, they may end up competing for the IA role. The secret is to maintain planned systems audits while also securing resources to cover what is part of the consultancy branch. If these additional services are important, then management will have to be prepared to finance them. It is important not to sacrifice assurance work by diverting audit resources to carrying out client-expectation services.

7. Legislation This is an important component in the development of internal auditing:

- It may alter the audit role by providing additional work.
- It may bring into the frame competitors for the current audit contract.

- It may impact the status of internal auditing, e.g. any moves towards mandatory audit committees or for that matter mandatory IA.

New legislation should be considered and the effects anticipated. The audit strategy and business plan should take on board these additional factors in a way that promotes the continuing success of the audit function. This means that the CAE must resource the continual search for new legislation that affects the organization's control systems or impacts on the future of IA.

8. Corporate governance, risk management and control As suggested by the current definition of internal auditing, these three concepts now form the framework for the design and provision of the IA service. One major issue is the growth of risk committees that are being established by main boards along with the appointment of high-level chief risk officers, and the impact this has on the IA role. This is why the next three chapters deal with these topics.

Why Study the Past?

The past forms a foundation for the future. This is true for IA and we have suffered our full share of poor reputations. Recent developments tend to be based on the concept of lifting the audit profile to deal with complicated specialist high-profile areas/issues. This brings not only prestige but also the need to meet high expectations. It can only be achieved where the audit function is actively implementing a strategy with clear steps for enhancing professionalism. The ability to offer a wide range of services while still retaining a formal methodology steeped in professionalism will be the feature of the new IA department. It will be necessary to market the audit service for those managers who still hold the old-fashioned view of the profession as a ticking and checking function. Taking responsibility for reviewing parts of the risk management system is another strong possibility that is hard to resist. So long as a two-tier system with basic low-level audits and contrasting complicated reviews does not result in an imbalance, then this service differentiation will be one solution. The client may demand the basic fraud/probity work that falls within the expectation frame where managers wish gaps in control to be closed in a way that will not form a criticism of their role. This is in contrast to the systems approach that seeks to locate responsibility for risk management at management's doorstep. The CAE of the future will need the ability to balance these two major and sometimes conflicting considerations. Internal auditors are now consultants, reviewers, advisors, risk co-ordinators and investigators. However, we are still called 'internal auditors' and Sawyer has made it clear that a name change was considered but rejected and we decided to 'bow to historical precedent.'[9]

Summary and Conclusions

This first chapter of the Handbook takes the reader through the structure of the book and highlights the pivotal role of the IIA standards. We have also provided a brief snapshot of the development of the IA role as an introduction to the subject. Many of the points mentioned above are dealt with in some detail in the main part of the book, although it is as well to keep in mind the basics of IA while reading more widely. The concept of IA is really quite simple – it is the task of putting the ideals into practice that proves more trying. We have featured Sawyer's views in this chapter, which is why we close with another quote on the wide range of benefits from a good IA team:

IA can assist top management in:

- monitoring activities top management cannot itself monitor;
- identifying and minimizing risks;
- validating reports to senior management;
- protecting senior management in technical analysis beyond its ken;
- providing information for the decision-making process;
- reviewing for the future as well as for the past;
- helping line managers manage by pointing to violation of procedures and management principles.[10]

Whatever the new risk-centred jargon used to describe the audit role, much of the above benefits described by Sawyer remain constant. A worthwhile profession is based on clear principles and not just fancy jargon.

Chapter 1: Multi-choice Questions

1.1 The Chief Audit Executive is defined by the IIA as:
   a. The officer who reports to every audit committee meeting.
   b. The most senior person responsible for promoting risk management in the organization.
   c. The most qualified internal auditor in post.
   d. A senior position within the organization responsible for IA activities.

1.2 Which is the correct IIA definition of internal auditing?
   a. Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations.
   b. Internal auditing is an independent, assurance and consulting activity designed to add value and improve an organization's operations.
   c. Internal auditing is an independent, objective assurance and consulting activity designed to add value to an organization's operations.
   d. Internal auditing is an independent, objective assurance and consulting service designed to add value or improve an organization's operations.

1.3 Which is the odd one out?
   Audit consisted mainly of checking, with the probity visits tending to centre on:
   a. cash income
   b. stocks
   c. purchases
   d. petty cash
   e. staff complaints
   f. stamps
   g. revenue contracts
   h. and other minor accounting functions.

1.4 Insert the missing phrase:
   In the past, IA was seen as an integral component of the . . . . . designed to double-check accounting transactions. The idea was to re-check as many items as possible so as to provide this continuous audit.
   a. operational handbook
   b. internal checking procedures
   c. budgetary control
   d. performance measurement

1.5 Insert the missing phrase:
The importance of sound organizational systems came to a fore in the US where the Foreign Corrupt Practices Act passed in …… stated that an organization's management were culpable for any illegal payments made by the organization even where they claimed they had no knowledge of the payments.
a. 1997
b. 1987
c. 1956
d. 2003

1.6 Which is the most appropriate statement?
a. The ability to understand and evaluate complicated behaviour patterns of employees allows audit to assume wide scope.
b. The ability to understand and evaluate complicated systems of managerial and operational controls allows audit to assume wide scope.
c. The ability to understand and evaluate complicated accounting records allows audit to assume wide scope.
d. The ability to understand and evaluate complicated systems of compliance checks allows audit to assume wide scope.

1.7 Which is the most appropriate statement?
a. Many IA shops have now moved into risk-based auditing where the audit service is driven by the way the organization perceives controls.
b. Many IA shops have now moved into risk-based auditing where the audit service is driven by the way the organization perceives compliance.
c. Many IA shops have now moved into risk-based auditing where the audit service is driven by the way the organization perceives its auditors.
d. Many internal audit shops have now moved into risk-based auditing where the audit service is driven by the way the organization perceives and manages risk.

References

1. Sawyer Lawrence B. and Dittenhofer Mortimer A., Assisted by Scheiner James H. (1996) *Sawyer's Internal Auditing*, 4th edition, Florida: The Institute of Internal Auditors, p. 8.
2. Flesher Dale (1996) *Internal Auditing: A One-Semester Course*, Florida: The Institute of Internal Auditors, pp. 5–6.
3. Internal Auditing (2002) *Distance Learning Module*: Institute of Internal Auditors UK&Ireland.
4. Moeller Robert and Witt Herbert (1999) *Brink's Modern Internal Auditing*, 5th edition, New York: John Wiley and Sons Inc.
5. Flesher Dale (1996) *Internal Auditing: A One-Semester Course*, Florida: The Institute of Internal Auditors, p. 5.
6. Flesher Dale (1996) *Internal Auditing: A One-Semester Course*, Florida: The Institute of Internal Auditors, p. 7.
7. Vinten Gerald (1991) Unpublished material from Masters Degree Programme, City University Business School.
8. Sawyer Lawrence B. and Dittenhofer Mortimer A., Assisted by Scheiner James H. (1996) *Sawyer's Internal Auditing*, 4th edition, Florida: The Institute of Internal Auditors, p. 11.
9. Sawyer Lawrence B. and Dittenhofer Mortimer A., Assisted by Scheiner James H. (1996) *Sawyer's Internal Auditing*, 4th edition, Florida: The Institute of Internal Auditors, p. 10.
10. Sawyer Lawrence B. and Dittenhofer Mortimer A., Assisted by Scheiner James H. (1996) *Sawyer's Internal Auditing*, 4th edition, Florida: The Institute of Internal Auditors, p. 13.

Chapter 2

CORPORATE GOVERNANCE PERSPECTIVES

Introduction

Corporate governance is a term that, over the last two decades, has now found its way into popular literature. It has been described by Sir Adrian Cadbury as the way organizations are directed and controlled. This simple statement contains many profound elements including the performance/conformance argument. An organization's main task is to achieve the level of performance that it was established for. But at the same time, an organization must adhere to all relevant standards, rules, laws, regulations, policies and expectations that form a framework within which this performance must be assessed, which in turn may cause many difficulties in the real world. Our first reference to corporate governance comes from Ireland: 'Improved standards of corporate governance, like "motherhood" cannot be argued against. It is critical to a small economy like Ireland, which is seeking to develop business in the more sophisticated sectors, that we are seen to operate to high standards.'[1]

A widely reported case, involving a large law firm, recounts the pressures placed on the legal teams who were told to charge a set number of fee paying hours each month, which resulted in the routine falsification of timesheets to achieve this target. While the firm's performance was excellent, as measured in terms of income achieved, it broke many rules in its charging practices and even committed the criminal offence of false accounting. That is, there was little conformance with rules, procedures and so on. The firm's direction was weak in that it created a culture of abuse and control was lacking in that routine working practices broke many rules. Short-term gains in income were secured, while in the long run a great deal of damage was done to the firm's reputation when the scandal was uncovered. Likewise the accounts were based on irregular income practices. The firm's partners, investors, employees and everyone else connected with the entity expected a high return, so the pressures this expectation created built up to force otherwise perfectly respectable people to falsify their charge sheets. A cruder much more direct version of this type of problem follows:

> Plumbing the depths: When the bosses of a repair firm told their workers to 'pump it up' they weren't referring to the plumbing. The catchphrase was a reminder to inflate the bill by whatever means possible. Customers could count on the plumbers, electricians, and heating engineers from the Abacus company to turn a domestic drama into a crisis . . . staff were told to create phantom jobs, damage parts deliberately, replace perfectly good ones and even go shopping in their customers' time.[2]

This simple illustration can be multiplied many times in all major developing and developed economies to give an insight into the type of problem that undermines the foundations of both business and public services. Corporate governance codes and policies have come to be relied on to re-establish the performance/conformance balance to ensure integrity, openness and

accountability. The codes are supported by structures that promote these three ideals and the internal audit function is a key component of the structure. Internal audit has a further role in educating top management in the available solutions and to help develop tools and techniques in this respect. The internal auditor who has a sound grasp of corporate governance is best placed to play a major role in the drive to ensuring sustainability as well as success in all business and service sectors. Corporate governance is now a separate exam paper for the IIA.UK&Ireland study programme. Also, the Chartered Association of Certified Accountants (ACCA) has established a Corporate Governance and Risk Management Committee to address new developments in these areas. Note that all references to IIA definitions, code of ethics, IIA attribute and performance standards, practice advisories and practice guides relate to the IPPF prepared by the IIAs in 2009. The sections covered in this chapter are:

2.1 The Agency Concept
2.2 Corporate Ethics and Accountability
2.3 International Scandals and their Impact
2.4 Models of Corporate Governance
2.5 Putting Governance into Practice
2.6 The External Audit
2.7 The Audit Committee
2.8 Internal Audit
2.9 The Link to Risk Management and Internal Control
2.10 Reporting on Internal Controls
2.11 New Developments
Summary and Conclusions
Assignments and Multi-choice Questions

2.1 The Agency Concept

The main driver for corporate governance is based on the agency concept. Here corporate bodies are overseen by directors who are appointed by the owners, i.e. the shareholders. The directors formulate a corporate strategy to achieve set objectives and meet market expectations, and in turn, employ managers and staff to implement this strategy. A simple model sets out this relationship in Figure 2.1.



FIGURE 2.1 Corporate governance (1).

If everyone was totally competent and totally honest then the model in Figure 2.1 would work quite well. Directors oversee their managers while managers run the business through the other employees. To achieve published objectives, the directors set targets for their management team, authorize a budget and then establish a mechanism for measuring performance. All business activity feeds into the accounting system and the directors report the results back to their shareholders in the annual report on performance and accompanying final accounts. Shareholders check the overall performance and financial results each year and ensure that their investment is intact. They have a right to any dividends and may well see a growth in the value of their investment through strong share prices. Meanwhile, the directors have a duty to take all reasonable steps to protect the business and account for their activities. The Stewardship concept means directors owe this responsibility to the parties who have a vested interest in the organization. They work for and on behalf of their masters, and need to demonstrate competence, which is not always easy. The view that directors are not always competent in understanding their responsibilities is illustrated by the following article:

> Many directors have virtually no idea of their powers, or of the legal obligations that they face . . . Examples of rules directors commonly break – either deliberately or unintentionally – include: borrowing money from companies over which they exercise control; failing to hold and minute board meetings as and when required by law; failing to declare an interest in contracts that involve the company; blindly battling to save a company in difficulties or technically insolvent when this presents a risk to the creditors; failing to understand the 'five year' directors' employment contract rule.[3]

There are two further mechanisms that need to be included in our model to reflect both the performance and accountability dimensions that are important in agency theory. This is a further aspect of the performance/conformance concept that has already been discussed, that is strategic performance measures and published accounts in Figure 2.2.

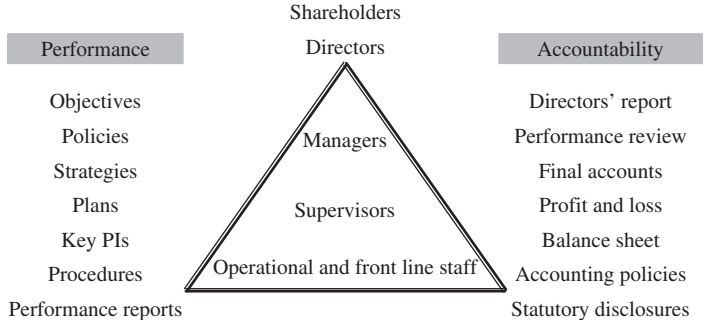


FIGURE 2.2 Corporate governance (2).

The standard performance accountability model needs three further refinements to ensure the proper running of business. These are shown in Figure 2.3:

- legislation and regulations;
- external publication of the final accounts prepared by the board;
- a strong set of ethical standards.

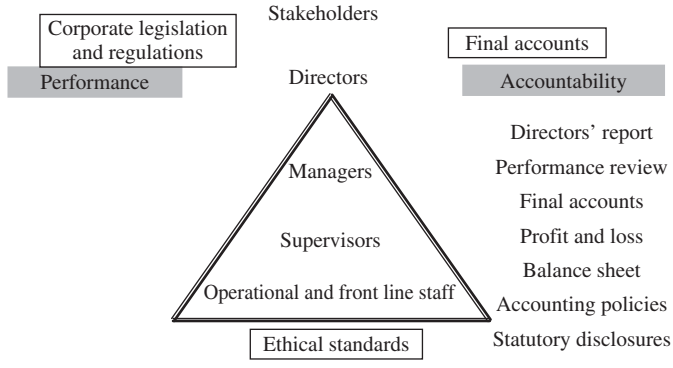


FIGURE 2.3 Corporate governance (3).

There are a raft of laws such as maximum working hours, minimum wage, anti-discrimination, consumer protection, anti-competition, insider trading, and health and safety along with company regulations set by the Department of Trade and Industry (DTI) and the Stock Exchange to guide the way business is conducted and the way people are treated. Final accounts are checked by an external firm of accountants to ensure they show a true and fair view of the company's financial performance and position. Most organizations have a set of ethical standards that are made clear to employees and others which help define unacceptable conduct. In this way, the growth, stability and demise of businesses is essentially dependent on the free flow of funds along with fair and open competition. The fittest companies survive while the less able must change, collapse or be consumed by stronger enterprises. The above model is straightforward and well understood as the proper basis for a capitalist system. The public sector is catered for by replacing the board with the accounting officer (for central government bodies) or chief executive for local authorities and other public service organizations. Not-for-profit organizations would have a similar responsible person at the helm. For public bodies, the owners are the taxpayers and the external auditors have an additional role in assessing performance and VFM as well as verifying the financial statements. In this way, public sector service strategies and performance measures are validated in the absence of the private sector profit motive. Again, a fairly simple model of corporate accountability. Unfortunately, there are certain flaws in this standard model, many of which hinder the degree of reliance that can be placed on the reports and representations published by large organizations. These potential problems include:

- Boards dominated by the chief executive officers (CEO) who manipulate the companies to their own personal agenda.
- Boards that are ineffectual and consist simply of a network of friends who fail to represent the shareholders to any real extent.
- Boards that are incompetent and meet on an irregular basis and simply rubber stamp the position set by the CEO or a small group of dominating board members.
- CEOs and chief finance officers (CFO) who conspire with other board members to distort the published results of the company for reasons of personal gain or because of a fear that a fall in the share price will strip the value of shares and options they hold in the company, particularly where the market expects instant and large returns in rapid growth business sectors.

- Employees who are regularly able to abuse company systems and exploit loopholes again for personal gain.
- Significant business ventures, take-overs and development projects that involve huge shifts of resources and large returns for entrepreneurs but which involve major risks that have not been fully addressed.
- Short-term measures such as dumping waste, skipping important safety checks or exploiting third world labour and resources that reap significant returns but involve illicit hardship to third parties. Many of these acts then being concealed through misreporting or cover-ups.
- Organizations with great emphasis on success where bad news is not tolerated and losses, problems, errors or breach of procedure are either ignored or concealed.
- One-dimensional performance targets where operations are inappropriately skewed towards quick wins or figures are massaged to produce predetermined results.
- Organizations where accountabilities have not been properly established and where a blame culture means certain employees are unfairly targeted.
- External audit routines that are designed to protect top management where the in charge audit partner has a basic allegiance to the company directors, particularly the CFO – who in reality determines the auditor's employment prospects, fees and extra consulting work.

In general, the basic model fails to ensure that the risks of all the above have been assessed and addressed to ensure they are unlikely to materialize. The normal performance/accountability model assumes people are competent and honest and takes no account of the fundamental pressures in society to place self-interest above absolute legitimacy. It also does not acknowledge the view that all players may not be competent to understand and fully discharge their set responsibilities. The growth and pace of big business, government reforms and global competition has led to a cut-and-thrust climate where individuals are either required to achieve instant success or at least give the appearance of having done so. High ethical standards which used to act as the glue that holds everything in place are now more like the glue that slows everything down and means a second rather than first place medal. Competence, clarity of roles and the proper discharge of professional obligations is a good ideal. However, a two-year study by the Royal Society of Arts (Corporate Governance in the Public and Voluntary Sector) concluded: 'The report also found that there is confusion among many board members about roles, responsibilities, managerial hierarchy and levels of authority as well as the legislative framework that defines and sets limits for their activities.'[4]

In a bid to rectify these types of problems, Corporate Governance is the enhanced (and codified) process that is superimposed over the basic performance/accountability model to try to counter the above problems. It is constructed in recognition of the need to encourage business performance, demonstrate that this performance is really earned and to encourage more openness in assessing the reported results. Moreover, it is founded on good business sense as a way of promoting sustainable and realistic growth and enhanced corporate performances.

Defining Stakeholders

The enhanced model in Figure 2.3 has changed the one-dimensional concept of *Shareholders* to the wider concept of *Stakeholders*. Most commentators argue that corporations need to acknowledge a wide range of people and groups affected by their operations and presence. Andrew Chambers has devised a 'Court of public opinion' as consisting of key figures including:

Customers	Regulators
Financiers	Business partners
Politicians	Shareholders
The media	Competitors
Employees	Government
Business leaders	Local communities[5]

The Institute of Directors (IoD) has published its views on stakeholder responsibility on their website:

> The IoD standards for the board state that the key purpose of companies is to maximize the efficient creation of wealth, while observing the law and seeking to minimize the negative impacts of corporate activity on participants and society generally. It follows therefore that the key purpose of the board of directors is to seek to ensure the prosperity of the company by collectively directing the company's affairs, while meeting the appropriate interests of its shareholders and relevant stakeholders and taking into account the laws, relevant regulations and commercial considerations.[6]

Many companies, such as TelecomAsia, publish their responsibilities to stakeholders as well as shareholders: 'Mission – To provide the best quality telecommunication and multimedia interactive services while satisfying customers, benefiting society, enriching the well-being of our employees and ensuing optimal returns to our stakeholders.'[7]

A recognition of the local community is also on the agenda of many larger companies as illustrated by British Petroleum PLC:

> We believe it is essential to conduct our business with integrity by upholding local laws, keeping our promises and commitments, practising business in an honest and upstanding manner, refraining from coercion and never deliberately doing harm to anyone. Those working on behalf of the BP group are expected to conduct business in a forthright manner and respect the dignity and rights of the people in the communities where we operate.[8]

This does not mean the shareholders can be sidelined in preference to all groups that come into contact with an organization. Shareholders have a right to have their investment managed with care and should expect some return (dividends) from the enterprise. They can vote on important matters such as who should be in charge of the company and how much they should receive for this task. Companies are paying much more attention to the needs of the shareholders and as one commentator states:

> Twenty years ago management had scant if any regard for shareholders, unless they were part of the family! In the 1980s two things happened. Once management thought they had better start talking to investors because they could sack the board. Then we had firms being bid for and normally they weren't the ones which had achieved much. As they tried to defend what they had done, you heard the great cry of short-termism which really meant – we failed to perform for the last three years but don't worry, we will do for the next three. Suddenly the bulb went on in our brains that we had power and could influence management. Boards also recognised they had to talk to their shareholders. Today we do have sensible dialogues.[9]

Providing lots of information to the shareholders may represent good intentions but at times information alone may not be enough:

> Royal Bank of Scotland's annual report, published this week, devoted seven pages to executive pay. Barclay's report has eight if you count the page on directors' pay. Every year, it gets harder for the reader to have a clue what is really going on. It is now virtually impossible to grasp how generous these schemes could be. Even remuneration consultants who devise them admit to being frequently baffled, at least when trying to unpick them on the basis of the information published in the annual report.[10]

In general, there are two types of stakeholders: those that have a direct *influence* on the organization's future activities such as investors, customers, regulators and shareholders; and those that simply have an *interest* in the organization, such as local community groups and journalists. It is the stakeholders who are affected by the way corporations behave. In a sense, this means almost everyone in society is affected by private corporations, listed companies and public sector bodies. Many argue that in the long run the interests of shareholders and general stakeholders tend to coincide so that all sides can be catered for via a single corporate strategy. The current view of corporate governance is that most capital markets across the world are dependent on the extent to which new codes and measures actually work. Section 2.3 addresses the fallout where things go wrong. When major scandals rock economies on both sides of the Atlantic, public confidence can be shaken to the bone.

2.2 Corporate Ethics and Accountability

The first question to ask is whether we need to establish corporate ethics within organizations? A survey by Management Today and KPMG Forensic Accounting of more than 800 directors, managers and partners illustrates why ethics needs to be considered in the working life:

- More than 2 out of 3 say that everyone lies to their boss on occasion.
- Less than half consider the people at the top to be strong ethical role models.
- Over 20% felt it was okay to surf the net for pleasure during work time.
- Around 25% would not say that favouring friends or family in awarding contracts was totally unacceptable.
- Some 7% agreed it was okay to artificially inflate profits so long as no money was stolen.
- Only 1 in 5 was prepared to say that charging personal entertainment to expenses was totally unacceptable (less than 15% for board directors).
- People over 40, those in financial positions and those in the public sector take a more judgemental approach to ethical behaviour.
- A dishonest member of staff may receive a clean reference from 3 in 10 managers.
- Reasons for not reporting a fraud include – alienate myself, none of my business, jeopardize my job, everybody's doing it, it is fair game.
- Nearly 10% of board directors say it is acceptable to massage their profit figures as long as no money is stolen.[11]

The immediate impact of poor ethical standards is demonstrated in the following story of the demise of one small business owner: 'The garage owner who sold Britain's most expensive petrol during the fuel crisis has gone bust after being boycotted by his customers, it emerged yesterday.'[12]

The Reith Lectures

For a clear position on ethics, we need go no further than the Reith lectures, which were inaugurated in 1948 by the BBC to mark the historic contribution made to public service broadcasting by Sir John (later Lord) Reith, the corporation's first director-general. Selected extracts from the Reith Lecture on Trust, number two, 2002 (presented by Onora O'Neill) follow:

> Real Accountability? – Perhaps the present revolution in accountability will make us all trustworthier. Perhaps we shall be trusted once again. But I think that this is a vain hope – not because accountability is undesirable or unnecessary, but because currently fashionable methods of accountability damage rather than repair trust. If we want greater accountability without damaging professional performance we need intelligent accountability. What might this include? Let me share my sense of some of the possibilities. Intelligent accountability, I suspect, requires more attention to good governance and fewer fantasies about total control. Good governance is possible only if institutions are allowed some margin for self-governance of a form appropriate to their particular tasks, within a framework of financial and other reporting. Such reporting, I believe, is not improved by being wholly standardised or relentlessly detailed, and since much that has to be accounted for is not easily measured it cannot be boiled down to a set of stock performance indicators. Those who are called to account should give an account of what they have done and of their successes or failures to others who have sufficient time and experience to assess the evidence and report on it. Real accountability provides substantive and knowledgeable independent judgement of an institution's or professional's work.[13]

Temptation

The next stage in the debate is to set out the reality of temptation that is placed in front of many professionals. A survey of procurement practitioners suggested that some 69% said that purchasers need to be more aware of ethics than other functions, while around 88% felt that purchasers' awareness of ethics had increased in the past five years. In terms of policies, 28% always take a potential supplier's ethics policy into account, in contrast to the 24% who never do so. Just over half of procurement practitioners had been offered a bribe by a supplier.[14]

Against this background, there is much that can go wrong when corporate ethics falls over. A few simple examples will help illustrate this fact:

> The fashion industry has long believed that the thinner and younger, the better. But last night, in the wake of serious concerns about sexual exploitation and drug abuse, the world's biggest model agency announced it will ban girls under 16 from cat walks and fashion shoots. In what could be a milestone for the industry, the Elite group in New York said it would no longer 'hire out' models under 16, even though some of the most successful girls make a fortune well before then. The move follows a BBC investigation into alleged under-age sex and drugs in the agency's European sister company, Elite Europe.[15]
>
> Wall Street giant Merrill Lynch agreed to pay a £70m fine and to impose strict controls on its share-tipping to settle a New York state probe into allegations that it misled investors with tainted research . . . it was alleged some of Merrill's 'buy' recommendations were influenced by the desire to drum up lucrative business from the firms concerned.[16]

Gifts can be used to disguise bribes and criminal activity, and can be hard to isolate. They can consist of a variation of:

Buying property below market value	Cash
Fashion vouchers	Free holidays
Gifts of wine	Lavish entertaining
Luxury hotels and trips abroad	Personal items for spouse
Purchases for below market value	

The Impact of Good Codes

Conversely, there is much that can be gained where a strong ethical foundation is in place:

> The pharmaceutical company mentioned in the COSO report was Johnson and Johnson. In the 1980s it faced a massive crisis when a malefactor inserted a deadly poison in bottles of one of its widely distributed products. The company had to decide whether to treat this as an isolated incident or take more drastic corrective action. Using its statement of ethical values as justification to recall and pull the entire product line, it averted a more serious crisis and received favourable publicity for its action.[17]

Ethical Codes

There are many different codes that have been developed to suit various organizations. These codes cover conduct, gifts, objectivity, honesty and so on. Adrian Cadbury has written about company codes:

> Turning now to company codes, they are drawn up to provide guidance to employees. They aim to assist those working in a company to know what standards of conduct are expected of them and how to deal with the kind of problems which they may come across in the course of their duties. Thus they need to be individually drafted, preferably with an input from those to whom they will apply. From a company's point of view, codes of conduct are a form of safeguard for their reputation.[18]

Some examples of ethical codes follow:

Civil service code This code constitutes a detailed set of provisions covering the conduct of civil servants and covers most areas of concern, including the need for impartiality. Selected extracts follow:

> Civil servants should conduct themselves with integrity, impartiality and honesty:
>
> - They should give honest and impartial advice to the Minister without fear or favour, and make all information relevant to a decision available to them.
> - They should not deceive or knowingly mislead Ministers, Parliament, the National Assembly or the public.
> - Civil servants should endeavour to deal with the affairs of the public sympathetically, efficiently, promptly and without bias or maladministration.
> - Civil servants should endeavour to ensure the proper, effective and efficient use of public money.
> - Civil servants should not misuse their official position or information acquired in the course of their official duties to further their private interests or those of others.
> - They should not receive benefits of any kind from a third party which might reasonably be seen to compromise their personal judgement or integrity.

- Civil servants should conduct themselves in such a way as to deserve and retain the confidence of Ministers.
- They should comply with restrictions on their political activities.
- The conduct of civil servants should be such that Ministers, Assembly Secretaries and the National Assembly as a body, and potential future holders of these positions can be sure that confidence can be freely given, and that the Civil Service will conscientiously fulfil its duties and obligations to, and impartially assist, advise and carry out the lawful policies of the duly constituted Administrations.
- Civil servants should not without authority disclose official information which has been communicated in confidence within the Administration, or received in confidence from others.
- Nothing in the Code should be taken as overriding existing statutory or common law obligations to keep confidential, or to disclose, certain information.
- They should not seek to frustrate or influence the policies, decisions or actions of Ministers, Assembly Secretaries or the National Assembly as a body by the unauthorized, improper or premature disclosure outside the Administration of any information to which they have had access as civil servants.
- Where a civil servant believes he or she is being required to act in a way which: is illegal, improper, or unethical; is in breach of constitutional convention or a professional code; may involve possible maladministration; or is otherwise inconsistent with this Code; he or she should report the matter in accordance with procedures laid down.
- A civil servant should also report to the appropriate authorities evidence of criminal or unlawful activity by others.
- Civil servants should not seek to frustrate the policies, decisions or actions of the Administrations by declining to take, or abstaining from, action which flows from decisions by Ministers, Assembly Secretaries or the National Assembly as a body.
- Civil servants should continue to observe their duties of confidentiality after they have left Crown employment.[19]

The National Health Service(NHS) There are many issues relating to the conduct of health trusts and medical staff regarding the degree to which the public are able to trust the National Health Service (NHS). One article illustrates the difficulty in achieving complete openness in the NHS:

> Doctors are still reluctant to tell patients when they make an error, despite warnings that they could be struck off if they try to bury their mistakes. Four out of ten specialists surveyed for a study, published in the British Medical Journal said they did not believe patients should always be told when a complication occurred and two thirds did not agree that the patient should be given detailed information about the possible consequences. In contrast, more than nine out of ten patients said they should be told about a mistake and more than eight out of ten said they would want to know what may happen as a result.[20]

There is in fact a code published by the NHS that addresses the issue of openness and it contains several interesting features. The aims of the code are to ensure that people:

- have access to available information about the services provided by the NHS, the cost of those services, quality standards and performance against targets;
- are provided with explanation about proposed service changes and have an opportunity to influence decisions on such changes;

- are aware of the reasons for the decisions and actions affecting their own treatment;
- know what information is available and where they can get it.

In implementing the Code, the NHS must:

- respond positively to requests for information (except in certain circumstances . . .);
- answer requests for information quickly and helpfully, and give reasons for not providing information where this is not possible;
- help the public know what information is available, so that they can decide what they wish to see, and to whom they should ask;
- ensure that there are clear and effective arrangements to deal with complaints and concerns about local services and access to information, and that these arrangements are widely publicized and effectively monitored.[21]

The Nolan principles This is a set of standards that cover people in public life, be they ministers, civil servants or people working in the wider public sector. The short but powerful set of seven principles can be used as the basis for developing a more detailed code for public sector organizations. There are seven standards in the Nolan code:

1. **Selflessness** – Holders of public office should take decisions solely in terms of the public interest. They should not do so in order to gain financial or other material benefits for themselves, their family or their friends.
2. **Integrity** – Holders of public office should not place themselves under any financial or other obligation to outside individuals or organizations that might influence them in the performance of their duties.
3. **Objectivity** – In carrying out public business, including making public appointments, awarding contracts or recommending individuals for reward or benefits, holders of public office should make their choices on merit.
4. **Accountability** – Holders of public office are accountable for their decisions and action to the public and must submit themselves to whatever scrutiny is appropriate to their office.
5. **Openness** – Holders of public office should be as open as possible about all the decisions and actions that they take. They should give reasons for their decisions and restrict information only when the wider public interest clearly demands.
6. **Honesty** – Holders of public office have a duty to declare any private interests relating to their public interests and to take any steps to resolve any conflicts arising in a way that protects the public interest.
7. **Leadership** – Holders of public office should promote and support these principles by leadership and example.[22]

The Link to Values

Most ethical codes are issued to staff and filed away, until they are updated. A better way to get ethics into the heart of business is to link them to corporate values, since values are about changing behaviours in a proactive manner. The role of values is described by Gareth Jones:

> Values are not a soft issue. Too many are quick to dismiss them as fads or corporate gestures – likening them to some damaging mission statements that state the boringly obvious. Used in the right way – not simply as a series of bon mots that hang like coded decorative wallpaper in the

> boardroom – values are a vital tool when used to bring about unity or a sense of purpose in a working world full of change and ambiguity. Values have the potential to do for employers what churches and pubs do for towns and villages. They offer a way of bringing the community together and building powerful common bonds.[23]

A value-based organization tends to have respect for employees, customers, suppliers and other stakeholders. This in turn promotes a more satisfied workforce and hopefully better all-round performance. The link between staff satisfaction and good performance has not always been fully established but there are those who are convinced that this is the case:

> Is there a link between employee satisfaction and a company's financial performance? New research from ISR suggests that there is. Companies which – compared with the industry in which they operate – achieve above-average net profits on invested capital, also have higher levels of employee satisfaction and commitment. Employees are not asked to sacrifice or compromise their personal standards and values in order to achieve organisational objectives. On the contrary, the best companies set an example for employees to aspire to. Employees are much more likely to believe that their company operates with integrity, both internally and externally.[24]

Implementing Ethics

Statements, codes and a recognition that corporate ethics underpins the value system of an organization are all good starters to ensuring business lives up to set standards. We need to go further in implementing suitable systems of corporate ethics so that the policies reach everyone in the organization (and those that are associated with it). Some years ago, the IoD developed the HUB programme to get ethics on the corporate agenda in a practical manner. The IoD said that:

> HUB is a long-term programme to change the culture and attitude of both business and its stakeholders by benchmarking business reputation. We need to find out how our stakeholders experience our business conduct. Our reputation is founded on the perceptions our stakeholders have of our business. The IoD HUB initiative sets out to enhance the reputation of business in Britain . . . HUB is:
>
> - Inclusive – measures perceptions of all stakeholders . . .
> - Translates values into action . . .
>
> HUB's aim is that by 2010 business and business people are respected and trusted to create wealth for the good of everyone, taking into account the interests of the wider community and conducting its operations with honesty, respect, trust, fairness, responsibility and innovation. HUB is based on three premises:
>
> 1. Investing in reputation is an investment with real return;
> 2. Good reputation is sustained by consistent standards of conduct and operations; and
> 3. Improving communication between a business and all its major stakeholders is a prerequisite to enhancing reputation.[25]

The International Dimension

Most larger companies have international links and associated business ventures. One dilemma is that standards set for domestic business may not be appropriate when dealing with overseas

business. It is a well known fact that many countries encourage some form of facilitation from large corporations from developed economies. Transparency International (TI) publishes an International Bribe Payers Index each year which lists the countries in order of propensity to require bribes from overseas companies. TI defines corruption as the abuse of public power for private gain and has listed the forces that encourage bribery. The changes and developments contributed to an increase in corruption by foreign companies of senior officials in the past five years – in order of significance:

- public tolerance of corruption
- deterioration of the rule of law
- immunity of high public office
- inadequate controls over money laundering
- low public salaries
- worsening public procurement practices
- increased secrecy in government
- privatization of state assets
- increased globalization and competition
- changes in political party funding
- increased financial liberalization
- restrictions on the media.[26]

It is now a criminal offence for UK companies to bribe overseas public officials under the Anti-Terrorism, Crime and Security Act, similar to the position for US companies. Most people agree that corruption has two sides – the offer and acceptance; and that companies that offer bribes simply encourage a continuation of corrupt practices. There is a subsidiary argument that at times, company officials have to offer inducements (described, for example, as local licensing fees) to have any chance of securing business abroad. The Organization for Economic Cooperation and Development (OECD) Convention on Combating Bribery of Foreign Officials led to the adoption of 17 Articles by OECD countries and five non-member countries on 21 November 1997. In addition, the OECD have developed Recommendation on Improving Ethical Conduct in the Public Service (April 1998) – which can be used to form the basis for an ethics management system:

- Ethical standards for public service should be clear.
- Ethical standards should be reflected in the legal framework.
- Ethical standards should be made available to public servants.
- Public servants should know their rights and obligations when exposing wrongdoings.
- Political commitment to ethics should reinforce the ethical conduct of public servants.
- The decision-making process should be transparent and open to scrutiny.
- There should be clear guidelines for interaction between the public and private sectors.
- Managers should demonstrate and promote ethical standards.
- Management policies, procedures and practices should promote ethical conduct.
- Public sector conditions and management of human resources should promote ethical conduct.
- Adequate accountability mechanisms should be in place with the public sector.
- Appropriate procedures and sanctions should exist to deal with misconduct.[27]

The propensity for public officials in less developed countries to promote the use of bribes and gifts as a way of life undermines the government sector and interferes with the ability to implement development reforms. It discourages international agencies to provide development

funds and loans, since corruption is seen to create a negative economic climate. Corruption thrives where there are poor controls, vague role definition and inconsistent authority lines. It also thrives where there are detailed rules and procedures for securing public services in place, since these tend to slow down the respective services, resulting in bribes being required to ensure whatever service needed is delivered speedily. In practice, the bribes are known as 'speed money' in some countries. In most cases, the control environment is extremely poor, with poor budgetary control, delays in procurement projects, no stock control, excessive delays caused by unwieldy procedures and excessive discretion by senior officials as well as badly trained staff (and recruitment based on nepotism). Many government officials are paid so little (some do not even receive their salaries on time) that there is an unwritten rule that income is made up with bribes. When this rule applies to law enforcement, the lines between criminals and police officers can become dangerously blurred. Companies that trade abroad need to ensure their ethics policies read across to the cultures that they operate within. The codes should be translated into relevant languages for local agents and the reasoning and benefits of a strong ethical position made clear. Ensure that the role of ethics officers is delegated to a suitable person based overseas and that local sensitivities are acknowledged and addressed as best as possible. There are areas of common concern and also OECD policies, and international law recognizes certain key principles that may be employed to good effect. The impact of poor accountability on development funding has always been a concern for the donor agencies. The United Nations has acknowledged this problem and one report from the Expert Group on Government Auditing concluded that:

> Clearly, imperfect accountability from host governments (or from other recipient institutions in host countries) undercuts the aid process. The normal reassurance that the money and other items provided, have been properly controlled and accounted for, and used for the purpose for which they were intended, are absent. Moreover, where accountability is seriously imperfect, donors find themselves ostensibly funding an agreed aid project when they are funding something completely different.[28]

Ethical Reporting

Roger Adams of the ACCA has put the case for corporate accountability reporting:

> The developments in corporate accountability over the past few years have heralded a new era in public reporting. Companies have come to realise that they are no longer assessed by financial performance alone. Reputation and self-preservation are important factors that are being increasingly considered by management. Companies often wish to be seen as doing the right thing . . . Nowhere is this more relevant than in the case of environmental and social issues. By incorporating these sorts of data in the annual report, companies add value to their corporate reports and communicate to a wider range of stakeholders.[29]

The growth in Social Ethical and Environmental (SEE) reporting has resulted in a code prepared by the Association of British Insurers on this topic, and extracts include that the board:

- takes regular account of the significance of SEE issues;
- identifies significant risks and opportunities arising from SEE issues;
- has adequate information and directors are trained in SEE issues;
- should ensure effective systems are in place to manage significant SEE risks.[30]

The annual report should:

- include information on SEE-related risks and opportunities;
- describe SEE risk management procedures;
- explain the extent to which the company has complied with its own policies on managing SEE risks;
- document procedures for verification of SEE disclosures.[31]

Some companies have taken a lead in ethical reporting. As an example, there follows a quote from the late Anita Roddick, from the Body Shop, and further material posted on the Body Shop website:

> I would love it if every shareholder of every company wrote a letter every time they received a company's annual report and accounts. I would like them to say something like 'Okay that's fine, very good. But where are the details of your environmental audit? Where are your details of accounting to the community? Where is your social audit?'[32]

Tesco, the retail company, have published their Corporate Social Responsibility Review (CSR) 2001/2002 on their website:

> The CSR strategy corresponds with the Tesco core Purpose and Values. We aim to set robust policies backed by a comprehensive programme and to communicate these effectively. We have a key accountability matrix which sets out the respective responsibilities of the departments and Directors for each area. We have divided our policies into three sections, Economic, Social and Environmental in accordance with GRI guidelines. Although we have divided our CSR policies into these categories, many of them, such as regeneration, straddle all three areas.
>
> 1. Economic Policies
> 2. Corporate Governance
> 3. Risk Management[33]

Whistleblowing

The Public Interest Disclosure Act 1998 applies to England, Scotland and Wales. Disclosures relate to crimes, breaches of legal obligations, miscarriages of justice, dangers to health and safety or the environment and concealing information relating to these items. Protected disclosures should be made:

- In good faith.
- Not for personal gain.
- Only after all relevant internal processes have been utilized.

The burden of proof for the above rests with the employee. Internal procedures can only be avoided where:

- employee believes s/he would be 'subject to a detriment' if disclosure made to the employer;
- evidence would be concealed by employer;
- employee has already made a disclosure of substantially the same information.

If internal procedures are unsafe then any official regulator should be informed (prescribed body). Public sector employees' information classified say under the Official Secrets Act does not benefit from the Public Interest Disclosure Act's protection. Gagging clauses are probably void under the Act. Employees dismissed as a result of protected disclosure should make representation to the employment tribunal within seven days of the dismissal. Neil Baker has described the Financial Services Authority's (FSA) Guidance for firms' whistleblowing policies:

- A clear statement that the firms take failures seriously. Failures in this context means doing something that a worker might want to blow the whistle about.
- An indication of what is regarded as a failure.
- Respect for confidentiality of workers who raise concerns, if they wish this.
- An assurance that, where a protected disclosure has been made, the firm will take all reasonable steps to ensure that no person under its control engages in victimisation.
- The opportunity to raise concerns outside the line management structure, such as with the compliance director, internal auditor or company secretary.
- Penalties for making false and malicious allegations.
- An indication of the proper way in which concerns may be raised outside the firm if necessary.
- Providing access to an external body such as an independent charity for advice.
- Making whistleblowing procedures accessible to staff of key contractors.
- Written procedures.[34]

There are well-known implications for whistleblowers as described in one example:

> Why I had to blow the whistle on heart unit – A hospital heart unit where 29 babies died put lives at risk in an attempt to keep its government funding, it was claimed yesterday. The doctor, who is generally credited with exposing the scandal of bungling operations at Bristol Royal Infirmary, said he tried to persuade bosses to halt some of the high-risk surgery. But the situation was like 'a train where the occasional passengers were falling off, and the train had to keep moving in order to attract funding' the consultant anaesthetist told a public inquiry into the scandal . . . he claims he was shunned by the medical establishment for making his disclosures and was forced to seek a job outside of Britain.[35]

Before the Public Interest Disclosure Act, the IIA.UK&Ireland had prepared what was then called a Professional Briefing Note Five (1994), covering whistleblowing which defined whistleblowing as:

> The unauthorized disclosure by internal auditors of audit results, findings, opinions, or information acquired in the course of performing their duties and relating to questionable practices.

Summary of points made:

- Internal auditors should act as good citizens and balance a number of issues in determining to whom and what they communicate.
- The briefing note is not a complete code on whistleblowing.
- Whistleblowing should not be necessary when the auditor acts in accordance with the IIA standards.
- Use all available authorized opportunities to communicate – this discharges the auditor's professional obligations.
- The auditor should consider resignation if appropriate.
- Auditors who go public have found it difficult to enter similar employment elsewhere.

Social Responsibility

Under the stakeholder concept, companies do have some responsibility to society over and above their stated intentions to make and invest money for the shareholders. The IoD has prepared a guide to CSR:

> in the absence of any specific duty outside company law to act in a specific way, acting in the interests of stakeholders could give rise to a legal challenge that they breached their fiduciary duties to the company . . . Since risk communication is fundamental to reputation management, Turnbull can provide companies with an effective mechanism for managing corporate reputation from the point of view of protecting brand and corporate identity . . . Companies face differing circumstances depending on their size and scope, and it is the directors of those companies who are most likely to appreciate the particular shareholder and stakeholder relationships they face, and who are best placed to make the necessary judgements. What is clear, however is that a growing number of boards are likely to judge that the concept of corporate responsibility and the issues arising from it, demand increasing attention.[36]

An old Professional Briefing Note (fifteen) on Ethics and Social Responsibility prepared by the IIA in 1999 is still relevant today. It described the importance of corporate reputation management and suggested that:

> It is probably the most important asset which is accumulated over time as the result of an organisation's conduct with regard to its relationships with its multi-various stakeholders, the quality, reliability and safety of its products or services, and its attention to social concerns as well as its contributions to the improvement of society. It is not enough to recognise the value of a good corporate reputation and to behave in ways directed towards achieving this. Reputations are the creation not of facts, but of perceptions. These perceptions must be managed, just like any other asset, they cannot just be left to speak for themselves. Reputation is made up of two dimensions. what it is, and how well it is known.

2.3 International Scandals and their Impact

Before we delve into the many cases that set the context for the training, codes, guides and regulations on corporate governance, it is as well to recall the words of Sir Adrian Cadbury in the run-up to the first major attempt to tackle concerns over poor accountability:

> The country's economy depends on the drive and efficiency of its companies. Thus the effectiveness with which their boards discharge their responsibilities determines Britain's competitive position. They must be free to drive their companies forward, but exercise that freedom within a framework of effective accountability. This is the essence of any system of corporate governance. (para. 1.1) By adhering to the code, listed companies will strengthen both their control over their business and their public accountability. In doing so, they will strike the right balance between meeting the standards of corporate governance now expected of them and retaining the essential spirit of enterprise. (para. 1.5)

Some of the more famous cases where these ideals have not been met are mentioned below:

Guinness – 1986

Ernest Saunders, the Chief Executive of Guinness, paid himself £3 million plus interest, and paid large sums to those who helped him rig shares in order to try and take over another drinks company, Distillers. He rigged the shares to beat Argyll, the company in competition with him to try and take over Distillers. Ernest Saunders was not alone in the share-rigging, senior businessmen from outside Guinness were also involved.[37] In fact, several other companies were associated with the problem and the implications were quite widespread. A government report into the Guinness take-over of Distillers, another drinks company, in 1986 took 11 years to prepare and cost taxpayers more than £2 million, revealed illegal share-rigging. The report also disclosed that Ernest Saunders, the former chief executive of Guinness, awarded himself a £3 million bonus, which he paid into a numbered Zurich bank account. The investigators, barrister David Donaldson QC and accountant Ian Watt, said: 'Ernest Saunders appeared to think he was entitled to his reward of £3 million plus interest after paying out "gargantuan sums" to the men who helped him create a phoney shares market. And he had therefore "voted" himself one without asking his board of directors.' Trade President Margaret Beckett said she had received strong legal advice that the individuals involved in the share-rigging were still free to sit on company boards as directors, and could not be disqualified from holding directorships. Instead, the Government is to look at ways of hardening up the role of financial watchdogs.[38] This scandal prompted the government of the day to look at ways of strengthening the role of financial watchdogs. The key figures in this scandal were right at the very top of the organization, so arguably, more junior members of staff working within finance may not even have been aware of what took place, let alone be able to question it.

Barlow Clowes – 1988

The Barlow Clowes business collapsed owing millions of pounds. The business was made up of a partnership and a company in the UK, with a total of 7,000 investors; partnerships in Jersey and Geneva, with 11,000 investors; and Barlow Clowes International in Gibraltar. From November 1985 until April 1987, Spicer and Oppenheim provided a range of services, including audit, but did not audit the businesses in Jersey or Geneva. The Joint Disciplinary Scheme (JDS) states that there was, in general, inadequate planning of the Barlow Clowes audit work and that: 'in many respects the audit work was poorly controlled and inadequately focused to ensure that reliable audit opinions could be drawn'. Money was also moved between client accounts as and when the need arose and spent without any regard to the rights of investors.

Peter Clowes moved approximately £100 million from the accounts of investors, and then spent it on planes, boats, jewellery and other things. In addition, £37 million pounds remained unaccounted for.[39]

In 1992, Peter Clowes, the founder and head of the Clowes businesses, was sentenced to ten years in prison.[40]

Polly Peck International – 1989

Asil Nadir was the head of Polly Peck International until its value dropped from £1 billion to less than half of that amount in 1989. The Stock Exchange had to suspend trading in Polly Peck International shares because of this fall in value. Asil Nadir was charged with false accounting and stealing a total of £31 million. There were also reports of insider trading. Asil Nadir fled to northern Cyprus in May 1993, shortly before his trial. Elizabeth Forsyth, Nadir's right-hand woman, however, was jailed for five years in March 1996 accused of laundering £400,000 Nadir allegedly

stole from shareholders to pay off his debts.[41] Elizabeth Forsyth felt confident after fraud charges against former Polly Peck chief accountant John Turner were dropped because it was unfair to try him in Nadir's absence.[42]

BCCI (Bank of Credit and Commerce International) – 1991

Bank of Credit and Commerce International (BCCI), regarded as the world's biggest fraud, caused a bank operating in over 60 countries worldwide, and supposedly valued at $20 billion, to become worthless. The bank collapsed in 1991 owing $13 billion. PricewaterhouseCoopers (PwC) has been criticized for not spotting that BCCI, which was founded in 1975, was almost certainly insolvent before 1977. This was ten years before PwC succeeded in becoming sole auditor of the bank over Ernst & Young. PwC, the external auditor, advised the Bank of England that the BCCI was riddled with fraud on 24 June 1991, and on 5 July 1991, the Bank of England shut BCCI.[43] Abdul Chiragh who prepared accounts for the company, was jailed for five and a half years in 1997 for preparing false accounts for offshore companies, which never traded and had no assets, to indicate they were financially sound, so Gulf Group shipping tycoon Abbas Gokal could borrow large amounts of money from the bank. Gokal was jailed for 14 years, fined £3 million and ordered to pay £4.3 million in costs.[44] In 1998 PwC, former auditor Ernst & Young, and the former majority shareholder of BCCI, the Sheikh of Abu Dhabi, paid Deloittes, BCCI's liquidator, £117 million in an out of court settlement. PwC did not accept blame, or admit liability for the exposed fraud. Abbas Gokal appealed against his sentence in 1999, claiming his conviction was unsafe, because he was arrested at Frankfurt airport en route to the US, where he had been offered immunity by the Manhattan District Attorney. Gokal also claimed that the judge, Mr Justice Buxton's summing up of the case at his original trial was unfair.[45]

Maxwell – 1991

Robert Maxwell, the founder and Chief Executive of the Maxwell publishing empire, manipulated funds to give the impression that the company was financially liquid, in order to disguise the fact that he had perpetrated a huge fraud, which came to light in 1991. The external auditors were Coopers & Lybrand.[46] The official report into the Maxwell scandal has revealed that long-term relationships between auditors and their client companies are to be prohibited. Hailed as the biggest shake-up of auditing in 100 years, accountancy firms will have to follow tough guidelines designed to prevent conflicts of interests and a willingness to turn a blind eye to dubious behaviour to retain lucrative contracts. Firms will be compelled to replace auditors after a set period, and the secondment of partners to sit on clients' boards will be banned. The changes may be the first major act of the tough new regulator, the Accountancy Foundation, which was set up as a result of this scandal, and started work in summer 2002.[47]

Baring Futures (Singapore) – 1995

Baring Futures Singapore (BFS) was set up to enable the Baring Group to trade on the Singapore International Money Exchange (SIMEX). Nick Leeson, an inexperienced trader, was employed to manage both the dealing and settlement office (front and back office). Leeson was unable to trade in the UK due to a false statement made to the regulatory body for financial traders, the Securities and Futures Authority. On appointment by BFS, he opened an unauthorized account, which he used to cover up his large trading losses, which remained undiscovered until Barings

collapsed in 1995.[48] BFS collapsed in 1995 owing approximately £850 million. Nick Leeson, rogue trader, was caught after absconding when his gambling on the derivatives market revealed a debt of about £800 million. The total amount lost by Leeson was about $1 billion. Leeson was able to conceal his huge losses due to a lack of internal controls in the system. Dutch Group ING bought up Barings after its collapse and bailed it out. Nick Leeson was convicted of fraud and sentenced to six and a half years in a Singapore jail in 1996. He served three and a half years of this sentence. Leeson is now out of jail.[49] Coopers & Lybrand, Barings auditors at the time, decided to sue nine of the bank's former directors and employees, blaming them for the collapse. The Bank of England took note of guidance from Arthur Andersen, which spent eight months compiling a report on supervision and concluded that more was needed. The Securities and Futures Authority is changing its rules to make senior executives more accountable for the misdemeanours of junior staff.[50]

Metropolitan Police – 1995

Anthony Williams, Deputy Director of Finance for the Metropolitan Police, was exposed as a fraudster. He stole £5 million over a period of eight years between 1986 and 1994 from a secret bank account, set up as part of a highly sensitive operation against terrorists. Anthony Williams was asked in the mid-1980s to set up the secret bank account. His signature was the only one required to authorize payments from the account, even though he had a co-signatory to the account. This enabled him to steal from the account to purchase homes in Spain, the South of England and Scotland, where he bought himself the title Laird of Tomintoul, and spent large amounts of money on property renovations. The internal controls in place were inadequate to manage the possible risks, and the external auditors failed to spot these risks early enough to prevent Williams perpetrating the fraud. The fraud was only discovered because a Scottish banker asked questions about the scale of Williams' spending on uneconomic renovations to his property in Scotland.[51] Williams was jailed for stealing £5 million over eight years. The Metropolitan Police described the Williams fraud as a 'one-off perpetrated by a clever, deceitful man who lived his life in compartments.'[52]

Sumitomo Corporation – 1996

Yasuo Hamanaka was a copper trader working for Sumitomo Corporation, the world's biggest copper merchant. 'The Hammer', as Hamanaka was known, was also known as Mr Five Per Cent, referring to the amount of the market he controlled on his own. He was the biggest 'player' in copper, selling about 10,000 tons a year and able to single-handedly sway prices. His early success, and the fact that he held such a large proportion of the market, allowed him to trade unchecked until it was too late. Yasuo Hamanaka was a rogue trader, who during ten years of double-dealing in Tokyo ran up losses of £1.2 billion. One senior manager said: 'This is probably the biggest loss you will ever see.'[53] In 1996, Yasuo Hamanaka admitted to unauthorized share dealing for over ten years, and running up debts of over £1 billion at Japanese conglomerate Sumitomo. Hamanaka was sentenced to eight years' imprisonment.[54]

Daiwa Bank – 1996

Between 1984 and 1995 Toshihide Iguchi made bad trades in the bond market at the Manhattan branch of Daiwa Bank. He covered up his bad trades by selling bonds from Daiwa's own accounts and forging documentation for the bank's files, to cover his tracks. He was in control of both the

front and back offices of the bank, in a small understaffed branch, where his activities remained unmonitored for 11 years. In 1995, when he could no longer cope, he wrote to his employers admitting that he had lost the bank $1.1 billion. He claimed he kept the level of debt to himself for so long because he had not wanted to let anyone down. In 1996, Toshihide Iguchi was convicted of fraud and falsifying documents and jailed for four and a half years in the US after losing the Daiwa Bank more than $1 billion in fraudulent trading over 11 years from 1984 onwards. Iguchi was ordered to pay $2.6 million in fines and restitution. Daiwa Bank paid $340 million in fines, and had to close all its businesses in America, after being sued by the US authorities. Also in 2000, 11 senior executives were ordered to repay a total of $775 million in damages to the Daiwa Bank. Kenji Yasui, the former president of Daiwa Bank's New York branch, was ordered to repay the bulk of the damages – a massive $500 million. The executives may appeal against the ruling.[55]

Morgan Grenfell – 1996

In 1996, it was revealed that Peter Young lost $600 million belonging to city bank Morgan Grenfell. Peter Young, as head of Morgan Grenfell's European Growth Unit Trust in 1995, a fund worth £788 million, became interested in buying shares in a company called Solv-Ex. Solv-Ex's US directors claimed to be able to extract oil from sand cheaply. Peter Young spent approximately £400 million of his company's money on Solv-Ex. He set up 'shell' companies in Luxembourg to buy Solv-Ex shares illegally. In 1996, Solv-Ex was under US federal investigation. By the time of his trial in 1998, Peter Young was declared mentally unfit. He attended court in women's clothing carrying a handbag. Morgan Grenfell was acquired by Deutsche Bank.[56]

Inland Revenue – 1997

Michael Allcock was group leader of the Inland Revenue's Special Office 2, investigating foreign businessmen's tax affairs between 1987 and 1992, when he was suspended from duty charged with fraud, accepting cash bribes, a lavish overseas holiday with his family, and the services of a prostitute, in exchange for information on cases. Allcock was jailed in 1997.[57] The Revenue's reform of the Special Compliance Office, as it is now renamed, now includes a confidential reporting system for outside professionals or individuals who suspect colleagues of dishonesty. Former taxman John Gwyer points out, there is still no whistleblowing system for outside professionals or individuals who suspect that a Revenue official may be corrupt. Five of Allcock's colleagues were demoted or disciplined after the Revenue's internal investigation. But none was dismissed, despite the seriousness of the case.[58]

Liberty National Securities – 1999

Martin Frankel was banned from securities trading after being unable to account for $1 million from a fund he managed in 1992. In 1999, Frankel set up an unlicensed brokerage Liberty National Securities and defrauded insurance companies in five American states out of more than $200 million by gaining controlling stakes in them before absconding. He was extradited from Germany to the US in 2001, and pleaded guilty to 24 federal charges of fraud, racketeering and conspiracy in 2002. Frankel could be imprisoned for 150 years and fined $6.5 million if he fails to cooperate with prosecutors to retrieve some of the money stolen. He used the money to finance his lavish lifestyle, to purchase expensive gifts for women, costly vehicles and large houses. When he was arrested in Germany in late 1999, he had nine passports and 547 diamonds. Martin Frankel is expected to be sentenced in 2003.[59]

Sellafield – 2000

Process workers were to blame for the scandal that hit Sellafield nuclear power plant and led to cancelled orders and the resignation of the chief executive. Process workers at the Sellafield nuclear plant falsified records measuring batches of fuel pellets processed from reprocessed plutonium and uranium. Safety inspectors gave managers at the plant two months to present an action plan to address their failures. The UK's nuclear watchdog, the Nuclear Installations Inspectorate (NII), focused on how the nature of the job, lack of supervision and poor training had contributed to the procedural failures. The data check was part of a quality assurance inspection, but the significance of the check had never been connected with safety, and was not emphasized to staff, so falsifying the data became a way of avoiding what staff saw as a pointless task.[60]

Equitable Life – 2001

Equitable Life is now an established financial scandal. Equitable Life gave contradictory information to savers, independent financial advisors and the media, and the regulator, the FSA, has refused to comment on its role in the disaster. When Equitable announced its cuts of 16% to pensions and 14% to other with-profits savings, the insurer implied the money would only come from promised terminal bonuses, leaving guaranteed bonuses and capital safe. In fact, Equitable Life is prepared to dig into both guaranteed bonuses and capital that people have saved in order to claw back the full 16%. So anyone who invested £100,000 with Equitable Life in autumn 2000 would be likely to walk away with just £77,000 a year on, instead of having the £104,000 that could have been expected. This has raised questions about the role of the regulator. An FSA spokesman said: 'It is up to investors to make their own investment decisions.' The FSA's hands-off approach appeared to be at odds with its responsibilities as outlined in the Financial Services and Markets Act. The Act says the FSA must take into account 'the needs that consumers may have for advice and accurate information'.[61] Equitable started selling guaranteed annuity rate (GAR) policies in 1956, but sold the last one in 1988, as an action group challenged its decision to cut GAR bonuses. The High Court ruled in Equitable's favour in 1999, but the Appeal Court overturned the High Court's decision in 2000. The House of Lords upheld the Appeal Court's decision, and 12 Equitable directors handed in their notice. In 2001, Halifax bought part of Equitable's operations for approximately £1 billion, and Equitable appointed Herbert Smith law firm to investigate its former board. In 2002 Equitable policyholders decided to forgo some of their rights in return for higher policy values, and Equitable sued its former auditor Ernst & Young and 15 former directors.[62] Policyholders contended that the FSA and the Treasury allowed Equitable to sell over 10,000 pension policies between 1998 and 2000, even though they knew the mutual's reserves were insufficient. The chairman of Equitable could not rule out further cuts in fund value.

Alder Hey – 2001

Police are conducting an enquiry into Dutch pathologist Professor Dick Van Velzen, who worked at the Alder Hey Hospital in Liverpool between 1988 and 1995. The scandal came to light when a mother discovered that when her child, who died at three months, was buried in 1991, all of his organs were not intact. Eight years later organs belonging to him were discovered at Alder Hey Hospital in Liverpool, and she held a second funeral service. But last year more body parts were discovered, and the bereaved mother held a third funeral service for her baby. The Government's

Chief Medical Officer Professor Liam Donaldson revealed that 10,000 hearts, brains and other organs were still being held at other hospitals across England, and that thousands of families remain unaware that the loved ones they buried have had organs illegally removed without their consent. These details were revealed by Professor Liam Donaldson in an official report on Alder Hey and into the scale of organ abuse in Britain.[63]

Enron – 2001

Enron, a multinational energy trading company based in Houston, Texas, collapsed when credit rating firms prepared to lower their assessments of the company's debt. Enron would have been compelled to repay loans gained on the basis of its loan rating, and faced weakened share price. Enron went from being worth $60 billion to bankruptcy. Enron collapsed because of its complicated trading activities and financial manipulation. The company's income came from buying and selling future prices of energy and other commodities. The amounts involved in the trades were shown incorrectly as income, rather than the marginal difference between each side of the transaction. Enron's actions were described as being akin to counting money it held temporarily on behalf of clients as all its own income. As well as responsibility for the external audit function, Andersen was also responsible for the internal audit at Enron.[64] Enron's collapse is much bigger than the demise of Polly Peck in 1989. Enron was America's seventh largest company. Directors hid the extent of Enron's liabilities, which led to bankruptcy and thousands of job losses. As the external auditor, Andersen is culpable in the collapse. John Ormerod argues: 'I think it's a mistake to look at audit on its own. You have to look at the whole framework of corporate governance.'[65] The company had made losses of $1 billion (£664.5 million). Andersen, the external auditor of Enron, was found guilty of obstructing justice on 15 June, due to its destruction of Enron documents. Andersen Worldwide, the umbrella group of Andersen globally, agreed to pay $60 million (£39 million) to Enron's creditors and investors. Late in 2002, Andrew Fastow, Chief Financial Officer of Enron, was indicted on 78 counts of conspiracy, fraud, money laundering and obstruction of justice which he denied. Michael Kopper, Fastow's assistant, pleaded guilty to conspiracy charges. In the same year, Timothy Belden, the former head of Enron, also pleaded guilty to one charge of conspiracy to commit fraud to manipulate energy prices, and agreed to cooperate with investigators as part of his deal with the government. As part of this deal, Belden could be jailed for five years and be fined up to $250,000 (£161,000).[66] Mr Fastow was formally charged on 31 October 2002.[67] It has now also emerged that 11 insurers claim JP Morgan used complex commodities deals to hide loans to Enron between 1998 and 2000. Certain e-mails relating to these derivatives transactions refer to them as 'disguised loans'. The New York judge, Jed Rakoff, who is to rule on whether the e-mails can be used by insurers fighting the $1 billion Enron-related lawsuit from the bank, said the use of the term: 'is an explosive one in the context of the case.'[68]

Just as the US economy was recovering from the Enron saga another huge scandal appeared in the form of WorldCom.

WorldCom – 2002

WorldCom was valued at $180 billion in 1999. The company was originally a small local telecommunications agency that grew very quickly into one of the largest providers in the industry. There was a change of senior management at WorldCom in 2002, who asked the internal auditor to examine particular accounting transactions. The internal auditor discovered

that corporate expenses were being treated as capital investments. That is, expenses were being set against long-term budgets, rather than being offset against profits immediately. This practice resulted in the inflation of WorldCom's profits and share value, creating the impression that the company was more valuable than it actually was.[69] WorldCom admitted coordinating one of the biggest accounting frauds in history in 2002 and inflating its profits by $3.8 billion (£2.5 billion) between January 2001 and March 2002. Six Enron directors associated with the fraud resigned in the US in December 2002. The Joint Disciplinary Scheme (JDS) will investigate the role of the now-defunct Andersen's London office in the shredding of documents.[70]

Allied Irish Bank (AIB) Allfirst (US Subsidiary) – 2002

Allfirst, Allied Irish Bank's (AIB) subsidiary, was based in Baltimore, Maryland, USA. In early 2002, AIB revealed that one of its traders, John Rusnak, had made transactions that resulted in a loss of almost $700 million (actual $691 million). Similar to the Barings scandal, Rusnak had been allowed to trade unsupervised for almost five years before the scale of his losses was discovered. Rusnak traded in what were regarded as low risk transactions, yet was able to run-up huge losses as AIB failed to oversee its Maryland activities as carefully as required. The Allfirst treasurer's conflicting responsibilities were in part responsible for this, as he was both accountable for trading profits and trading activities.[71] Rogue trader John Rusnak went on the run in 2002. Rusnak and his attorney finally contacted the FBI investigators looking into the fraud. Rusnak pleaded guilty to one count of bank fraud and agreed to a reduced sentence in return for helping the investigation into whether there were others involved in the fraud. He agreed to a seven and a half year jail sentence and five year probation. He would have faced up to 30 years' imprisonment and up to $1.1 million in fines if convicted. John Rusnak was jailed for seven and a half years in January 2003, after being convicted. In 2002, AIB agreed to sell Allfirst to the US bank M & T Corporation for around $3.1 billion, and will retain a 22.5% stake in the resulting bank.[72] As a trader with a large position in the falling market Rusnak had no option but to make margin payments each month. As the losses mounted, instead of hedging his losses by buying options, he developed a system of bogus options and allegedly pretended to make trades, which enabled him to make it appear that Allfirst's books balanced. He used the money saved to make the margin payments.[73] Eugene Ludwig, a former US banking regulator, published his report into Rusnak's £494 million fraud in March 2002. Ludwig's report into the Rusnak fraud highlights the basic mistakes that internal auditors are advised never to allow:

> These include a failure to carry out basic checks, a failure to follow up recommendations, a failure to verify information from independent sources, the inability to understand areas of the business that they were meant to audit, a failure to test key controls effectively and a reluctance to stand up to superiors who did not want to be audited.[74]

Xerox – 2002

The Securities and Exchange Commission, the US financial regulator, filed a suit against Xerox in April 2002 for misstating its profits to the tune of almost $3 billion. Xerox reached a settlement with the Securities and Exchange Commission (SEC) and agreed to pay a fine of $10 million, but neither denied or admitted any wrongdoing. The fine imposed by the SEC is the largest fine ever imposed on a publicly traded firm in relation to accounting misdeeds.[75]

Merrill Lynch – 2002

The investment bank was fined by New York attorney general Eliot Spitzer to the tune of $10 million in 2002. The bank's analysts were suspected of advising investors to purchase worthless stocks, so the former could then secure investment banking business from the businesses concerned. The settlement imposed by Spitzer did not require Merrill Lynch to admit guilt for its actions.[76]

Credit Suisse First Boston (CSFB) – 2002

The FSA, the UK's financial watchdog, fined Credit Suisse First Boston (CSFB), the US-based investment banking arm of Switzerland's Credit Suisse £4 million ($6.4 million) for trying to mislead the Japanese tax and regulatory authorities in 2002.[77] CSFB is expected to be fined $150–$250 million over biased investment advice allegations on Wall Street. The company was fined $100 million in December 2001 in settlement of alleged dotcom flotation abuses, and was banned in India for share price fixing. CSFB has also been ridiculed for asking staff to 'try to keep dinners below $10,000', and fined £540,000 in the UK in 2001, for misleading clients into buying loss-making products.[78] The FSA said the CSFB's London-based derivatives arm had concealed documents, bought a shredder and moved documents offsite to avoid an audit by Japanese authorities in an attempt to mislead them. The FSA also said CSFB had colluded to misinform the tax authorities. Carol Sergeant, Managing Director at the FSA, was clear about how seriously the watchdog viewed attempts to mislead regulators. Management at CSFB has since changed, and has issued a statement indicating that it takes its regulatory responsibilities very seriously.[79]

Note that some of the more recent scandals are discussed towards the end of this chapter.

2.4 Models of Corporate Governance

We have established the classical model of corporate accountability and the ethical frameworks that are being used by organizations to promote sustainability. The last section provided a frightening insight into the fallout when things go wrong. The ripples caused by corporate scandals have recently become strong waves of discontent as the search has been made for workable and lasting solutions. Most solutions come in the guise of codes of practice that have been documented and appear as regulations or guidance for relevant organizations. Companies listed on various international stock markets are meant to subscribe to listing rules or make clear their reasons (and the implications) for failing to observe the rules. Health Trusts fall under the guidance provided for NHS organization and central government bodies have reference to guidance issued by the Treasury. Local authorities again have their own set of guidelines on promoting corporate governance, set within the local democracy and accountability framework for their environment. Not-for-profit organizations will also have their own set of standards for these types of voluntary, charitable and community-based organizations. Smaller family-run companies will have less stringent provisions and in countries where family-run enterprises are the norm, there is less concern with rules designed for the agency/stewardship relationship that was mentioned earlier on. Whatever the format and whatever the country, there is a growing trend towards corporate governance standards to be part of the way business and public services are conducted. We deal with some of the more well-known codes in this section of the chapter. Before we start, the IIA have provided a definition of governance:

> The combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives.

The landmark 1992 Cadbury Report described corporate governance:

> The country's economy depends on the drive and efficiency of its companies. Thus the effectiveness with which their boards discharge their responsibilities determines Britain's competitive position. They must be free to drive their companies forward, but exercise that freedom within a framework of effective accountability. This is the essence of any system of corporate governance. (Para. 1.1)

Cadbury went on to document the simple but now famous phrase: 'Corporate governance is the system by which companies are directed and controlled' (para. 2.5).[80]

Note that a synonym for governance is *controlling*. The globalization of governance processes is bringing the world closer in terms of commonality. Hand in hand with international accounting standards, we are approaching an era of closer comparability throughout the developed and developing world and it is as well to refer to the non-binding OECD Principles of Corporate Governance, because it has a global context. The principles are based on a philosophy that codes should be concise, understandable and accessible. The aim is to help improve legal, institutional and regulatory framework as guidance to stock exchanges, corporations and investors. They see corporate governance as a set of relationships for company management, the board, shareholders and stakeholders and setting objectives and monitoring performance in the context of the separation of ownership and control. They also make the point that corporate ethics and societal interests can affect the company's reputation and impact on the long-term success in attracting investors and 'patient' long-term capital through clear and understandable provisions. The OECD recognizes that there is no single good model of corporate governance (CG) and that the principles are evolutionary and change with innovation in corporations. There are five key principles involved, summarized as follows:

1. **Rights of shareholders.** CG framework should protect shareholders' rights.
2. **The equitable treatment of shareholders.** CG framework should ensure the equitable treatment of all shareholders, including minority and foreign shareholders.
3. **The role of stakeholders in corporate governance.** CG framework should ensure that timely and accurate disclosure is made of all material matters regarding the corporation, including the financial situation, performance, ownership and governance of the company.
4. **Disclosure and transparency.** CG framework should ensure that timely and accurate disclosure is made on all material matters regarding the corporation, including the financial situation, performance, ownership and governance of the company – includes financial and operational results, company objectives, share ownership and voting, board membership and remuneration, material foreseeable risk factors, governance structures and policies and annual audit and access to information by users.
5. **Responsibility of the board.** CG framework should ensure the strategic guidance of the company, the effective monitoring of management by the board, the board's accountability to the company and the shareholders. The board should be fully informed, fairly treat shareholders, ensure compliance with laws etc., review performance and risk policy etc., also ensuring that appropriate systems of internal control are in place, in particular, systems for monitoring risk, financial control and compliance with the law and disclosure and communications. Board should consider using NEDs and have access to accurate, relevant and timely information (and access to key managers such as company secretary, and the **internal auditor** and recourse to independent external advice).

While these are fairly general in nature because of their global application, the principles do provide a good foundation for country-specific codes. One phrase that is often used by proponents of corporate government is that 'a one size fits all model will not work in practice'. Moreover, there is no point listing a set of rules that can be ticked off and filed under 'Job Done!' There needs to be a constant search for principles that set the right spirit of enterprise that has not run wild. European Union regulations mean member states' listed companies will have to adopt International Accounting Standards by 2005 and this will bring Europe closer to becoming a single equity market.

The UK Experience

Cadbury The development of corporate governance in the United Kingdom provides a remarkable synopsis of the topic as it has evolved and adapted, slowly becoming immersed into the culture of the London business scene. One summarized version of this development (drawing on an account of Sir Adrian Cadbury's involvement after his report had been out for ten years) appears as follows:

> Two important cases hit the headlines over a decade ago (Coloroll and Polly Peck) where major problems were concealed in the accounts presented to shareholders, investors and the City. In May 1991 the London Stock Exchange, the Financial Reporting Council and accountancy bodies commissioned Cadbury and other committee members to review the problems and ensure confidence in the London markets was not damaged at all. This was the first opportunity for the business community to engage in a serious and open debate on the topic of governance and accountability. Just as the committee got to work, the BCCI and Maxwell cases broke and the committee's work took on a much higher profile, as London's reputation as a reliable trading centre was severely dented. The Cadbury report appeared to a barrage of protest as the business community felt attacked by rafts of new regulations. The 19 items in the code represent best practice guides that at first were resisted by several listed companies. The Code covers 19 main areas:
>
> [1] The board should meet regularly, retain full and effective control over the company and monitor the executive management.
> [2] There should be a clearly accepted division of responsibilities at the head of a company, which will ensure a balance of power and authority so that no one individual has unfettered powers of decision.
> [3] The board should include non-executive directors of sufficient calibre and number for their views to carry significant weight.
> [4] The board should have a formal schedule of matters specifically reserved to it for decision to ensure that the direction and control of the company are firmly in its hands.
> [5] There should be an agreed procedure for directors, in the furtherance of their duties to take independent professional advice if necessary at the company's expense.
> [6] All directors should have access to the advice and services of the company secretary, who is responsible to the board for ensuring that board procedures are followed and that applicable rules and regulations are complied with.
> [7] Non-executive directors (NED) should bring an independent judgement to bear on issues of strategy, performance, resources, including key appointments and standards of conduct.
> [8] The majority of NEDs should be independent of management and free from any business or other relationship which could materially interfere with the exercise of independent judgement, apart from their fees and shareholdings.
> [9] NEDs should be appointed for specified terms and re-appointment should not be automatic.

[10] NEDs should be selected through a formal process and both this process and their appointment should be a matter for the board as a whole.
[11] Directors' service contracts should not exceed three years without shareholders' approval.
[12] There should be full disclosure of a director's total emoluments and those of the chairman and highest paid UK directors.
[13] Executive directors' pay should be subject to the recommendations of a remunerations committee made up wholly or mainly of NEDs.
[14] It is the board's duty to present a balanced and understandable assessment of the company's position.
[15] The board should ensure that an objective and professional relationship is maintained with the auditors.
[16] The board should establish an audit committee of at least three NEDs with written terms of reference which deal clearly with its authority and duties.
[17] The directors should explain their responsibility for preparing the accounts next to a statement by the auditors about their reporting responsibilities.
[18] The directors should report on the effectiveness of the company's system of internal control.
[19] The directors should report that the business is a going concern, with supporting assumptions or qualifications as necessary.

Implicit in the code are several key considerations:

- the need to split the boardroom roles of chair and chief executive to ensure the dominance that was a feature of the Maxwell case less likely.
- the need to stop the unfettered abuse through excessive and unstructured directors' remuneration and benefits.
- the need to ensure there are good controls in operation.
- the need to ensure better oversight through an audit committee of NEDs.

Cadbury went on to describe the underpinning principles behind the code:

1. **Openness** – on the part of the companies, within the limits set by the competitive position, is the basis for the confidence which needs to exist between business and all those who have a stake in its success. An open approach to the disclosure of information contributes to the efficient working of the market economy prompts boards to take effective action and allows shareholders and others to scrutinise companies more thoroughly.
2. **Integrity** – means both straightforward dealing and completeness. What is required of financial reporting is that it should be honest and that it should present a balanced picture of the state of the company's affairs. The integrity of reports depends on the integrity of those who prepare and present them.
3. **Accountability** – boards of directors are accountable to their shareholders and both have to play their part in making that accountability effective. Boards of directors need to do so through the quality of information which they provide to shareholders, and shareholders through their willingness to exercise their responsibilities as owners.[81]

Rutteman The 1993 working party chaired by Paul Rutteman considered the way the Cadbury recommendations could be implemented. The draft report was issued in October 1993 and retained the view that listed companies should report on internal controls but limited this responsibility to internal financial controls. The final report issued in 1994 asked the board to report on the effectiveness of their system of internal control and disclose the key procedures established to provide effective internal control. In one sense, this was a step backwards in

that internal financial controls meant those systems that fed into the final accounts but did not extend the reporting requirements to the business systems that supported the corporate strategy. Reviewing, considering and reporting on internal financial controls does cost extra money but large companies have traditionally been examined by their external auditors. The task of reviewing financial controls was fairly straightforward although the need to assess and report on their 'effectiveness' posed some difficulty. This is because controls can never be 100% effective – sometimes, something may possibly go wrong. Corporate governance in focusing on the behaviour of the board and financial controls was headed for a back seat in business – which is more concerned with setting, implementing and driving strategy to produce the right results.[82]

Nolan Lord Nolan's 1994 standards in public life have been mentioned above. This forum was set up by the then Prime Minister to prepare codes for MPs, civil servants and people who are in public life, and reinforced the need to ensure a sound ethical base in the public sector, against the backdrop to allegations of sleaze and abuse that was a regular feature of the early 1990s. Also the new format of the civil service in the guise of departments, agencies, non-departmental public bodies (NDPBs) and other public bodies made it harder to ensure consistency in public behaviour. This committee was later chaired by Lord Neill and then Sir Nigel Wick and issues regular update reports to Parliament.

Greenbury As government was beset with problems of fees and cash paid to ministers by lobby groups and others, the City had a similar problem explaining why and how directors received what appeared to be excessive fees, bonuses and benefits (including options and special joining/leaving and pension arrangements). To address the mounting disquiet from stakeholders, the Richard Greenbury Committee was set up by the Confederation of British Industry (CBI) in 1995 to report independently on directors' earnings. The resultant report established a code of best practice in setting and disclosing directors' remuneration. Extracts from the Greenbury report include:

- To avoid potential conflicts of interest, Boards of Directors should set up remuneration committees of Non-Executive Directors to determine on their behalf, and on behalf of the shareholders, within agreed terms of reference, the company's policy on executive remuneration and specific remuneration packages for each of the Executive Directors, including pension rights and any compensation payments. (para. A.1)
- Boards should develop clear terms of reference for their remuneration committees. These should require the committee: (para. 4.4)
  a) to determine on behalf of the Board and the shareholders the company's broad policy for executive remuneration and the entire individual remuneration packages for each of the Executive Directors and, as appropriate, other senior executives;
  b) in doing so, to give the Executive Directors every encouragement to enhance the company's performance and to ensure that they are fairly, but responsibility, rewarded for their individual contributions;
  c) to comply with our Code of best practice;
  d) to report and account directly to the shareholders, on the Board's behalf, for their decisions.
- Remuneration committees' first concern should be with the remuneration of the Executive Directors. However, their remit may need to extend to other senior executives in the company even if they are not formally Executive Directors. (para. 4.5)
- The annual remuneration committee report to shareholders should be the main vehicle through which the company discloses and accounts to shareholders for Directors'

> remuneration. The report should be made on behalf of the Board. It should form a separate section within, or annexed to, the company's annual report and accounts. It should set out the company's general policy on executive remuneration and the actual remuneration packages, including share options and pension entitlements earned, of the individual Directors by name. The amounts received by, and committed to, each Director should be subject to audit. (Para. 5.4)[83]

Hampel The committee chaired by Sir Ronnie Hampel was set up in 1995 by the London Stock Exchange, the CBI, the IoD, Consultative Committee of Accountancy Bodies (CCAB), National Association of Pension Funds and the Association of British Insurers. This committee was the main successor to Cadbury and had the task of updating further the corporate governance debate and ensured the stated intentions of Cadbury were being achieved. They decided that while directors should review the effectiveness of internal control they need not report on the effectiveness of these controls. Internal audit was supported but not mandatory, although the need for an internal audit function should be reviewed annually. The final report was issued in January 1998 and also considered the role of shareholders and auditors. Paragraphs 6.11 to 6.13 provide an interesting account of the most crucial 'effectiveness' debate:

> The word 'effectiveness' has proved difficult both for directors and auditors in the context of public reporting. It can imply that controls can offer absolute assurance against misstatement or loss; in fact no system of control is proof against human error or deliberate override. There has also been concern that directors or auditors who confirm the effectiveness of a company's control system may be exposed to legal liability if unintentional misstatement or loss of any kind is found to have occurred. The report of the working group therefore recommended that the directors' statement should acknowledge the board's responsibility for the internal financial control system, but explain that such a system can provide only reasonable assurance against material misstatement or loss; should describe the key procedures established in order to provide effective financial controls; and should confirm that the directors had reviewed the system's effectiveness. Directors are also encouraged, but not required, to state their opinion on the effectiveness of their system of internal financial control. Relatively few companies have done this. (para. 6.11)
>
> It has been suggested that point 4.5 of the Cadbury code should be amended to read 'The directors should report on the company's internal control' – i.e. dropping the word 'effectiveness'. This would not require any change to the minimum requirements of the working group's effectiveness – the directors would still need to review the system's effectiveness. This would recognise what is happening in practice and seems entirely sensible. We believe that auditors should not be required to report publicly on directors' statements, but that they can contribute more effectively by reporting to directors privately. This would enable a more effective dialogue to take place; and allow best practice to continue to evolve in the scope and nature of such reports, rather than externally prescribing them. (para. 6.12)
>
> The working group refers to internal financial control, defined as internal controls over the safeguarding of assets, the maintaining of proper accounting records and reliability of financial information used within the business or for publication. But the guidance also encouraged directors to review and report on all aspects of internal control, including control to ensure effective and efficient operations and compliance with laws and regulations. We accept that it can be difficult in practice to distinguish financial from other controls: and we believe that it is important for directors and management to consider all aspects of control. We are concerned not only with the financial aspects of governance and we fully endorse the Cadbury comment that internal control is a key aspect of efficient management. Directors should therefore maintain and review controls addressing all relevant control objectives. These should include business risk

assessment and response, financial management, compliance with laws and regulations and the safeguarding of assets, including minimising the risk of fraud. (para. 6.13)

Combined code The recommendations provided by Cadbury and the later reviews of corporate governance were consolidated into what was known as the Combined Code in 1998. This code became part of the Stock Exchange listing requirements but still left a gap as the guidance was simply a mix of the previous guides. It also became clear that the corporate governance provisions had some relevance to organizations beyond listed companies.

Turnbull committee The ongoing saga of large company corporate governance was continued through the work of Sir Nigel Turnbull who prepared a short report in 1999. This working party was set up by the Institute of Chartered Accountants in England and Wales (ICAEW) in 1998 with support from the London Stock Exchange focusing on the internal control reporting provisions from the Combined Code. The final report in September 1999 was fairly brief and reinforced most of the sentiment from past work. The big leap confirmed the need to report across the business on statements of internal control (and not only the narrow financial controls), and linked this to the Committee of Sponsoring Organizations of the Treadway Commission (COSO) control framework (see the chapter on internal control) and underpinning risk assessment as a lead into sound controls. This report provided the foundation for the rapid growth in enterprise-wide risk management (see the chapter on risk management). In the words of Turnbull, the guidance is intended to:

- reflect sound business practice whereby internal control is embedded in the business processes by which a company pursues its objectives;
- remain relevant over time in the continually evolving business environment; and
- enable each company to apply it in a manner which takes account of its particular circumstances. (para. 8)

The guidance requires directors to exercise judgement in reviewing how the company has implemented the requirements of the Code relating to internal control and reporting to shareholders thereon. The guidance is based on the adoption by a company's board of a risk-based approach to establishing a sound system of internal control and reviewing its effectiveness. This should be incorporated by the company within its normal management and governance processes. It should not be treated as a separate exercise undertaken to meet regulatory requirements. (para. 9)

Selected extracts from the confirmed listed companies annual reporting requirements include the following:

- Principle D2: The board should maintain a sound system of internal control to safeguard shareholders' investment and the company's assets. (para. 2)
- Principle D2.1: The directors should, at least annually, conduct a review of the effectiveness of the group's system of internal control and should report to shareholders that they have done so. The review should cover all controls, including financial, operational and compliance controls and risk management. (para. 3)
- Principle D.2.2: Companies which do not have an internal audit function should from time to time review the need for one. (para. 4)
- A narrative statement of how it has applied the principles set out in Section 1 of the Combined Code, providing explanation which enables its shareholders to evaluate how the principles have been applied; (para. 5.a)

- A statement as to whether or not it has complied throughout the accounting period with the Code provisions set out in Section 1 of the Combined Code. (para. 5.b)
- The intention is that companies should have a free hand to explain their governance policies in the light of the principles, including any special circumstances which have led to them adopting a particular approach. (para. 6)[84]

The saga continues and we expect to see further codes appear in the UK as time goes by. In fact, Nigel Turnbull's view on this likelihood has been formally reported:

> The Turnbull report on internal control is likely to be reviewed in five years time according to Rank Group Finance Director, Nigel Turnbull, the chairman of the English ICA-backed working party behind the review. Speaking at the launch of the paper, which has been endorsed by the Stock Exchange as part of its listing requirements, Turnbull said it did not mark the end of the debate. 'In a five year timetable something new might easily emerge but if there are problems with the current paper, they may well get resolved in practice,' he said.[85]

One key concept behind Cadbury is based on getting the board to behave properly and be fully accountable to their shareholders. A further key concept behind the reporting aspects confirmed by Turnbull is based around the uncertainty factor inherent in systems of internal control. No system can guarantee the success of an organization. This is in spite of the efforts of consultants, auditors, risk management experts, executives and competent and motivated staff. A company cannot report that it will never experience a crisis, breakdown, fraud or a system collapse. It can only report that its systems are resilient and efficient enough to respond to most foreseeable risks and that they are kept up to date and as effective as possible. The controls therefore can only provide a reasonable expectation of ensuring corporate success just as external audit can only give a reasonable expectation of discovering material financial misstatement. The published report of any organization cannot really say anything else. Corporate lawyers get very concerned at the potential for claims against authors, reviewers and auditors who provide formal public statements on their ability to provide for all eventualities. The experience from the UK's attempts to meet this challenge on the premise that listed companies need to publish their position on internal control based on all reasonable (and competent) efforts is a cornerstone of good corporate governance. Moreover, those involved in creating the standards and codes have insisted that the underlying structures are derived from good business practice. They are part of good business and not a bureaucratic procedure that simply overlays the companies' real work. More recently, the Financial Reporting Council has prepared a revised Combined Code, extracts of which are reproduced below:

Section 1 Companies

A. Directors

A.1 The Board

Main Principle Every company should be headed by an effective board, which is collectively responsible for the success of the company.

Supporting Principles The board's role is to provide entrepreneurial leadership of the company within a framework of prudent and effective controls which enables risk to be assessed and managed. The board should set the company's strategic aims, ensure that the necessary financial and human resources are in place for the company to meet its objectives and review

management performance. The board should set the company's values and standards and ensure that its obligations to its shareholders and others are understood and met. All directors must take decisions objectively in the interests of the company. As part of their role as members of a unitary board, non-executive directors should constructively challenge and help develop proposals on strategy. Non-executive directors should scrutinise the performance of management in meeting agreed goals and objectives and monitor the reporting of performance. They should satisfy themselves on the integrity of financial information and that financial controls and systems of risk management are robust and defensible. They are responsible for determining appropriate levels of remuneration of executive directors and have a prime role in appointing, and where necessary removing, executive directors, and in succession planning.

A.2 Chairman and chief executive

Main Principle There should be a clear division of responsibilities at the head of the company between the running of the board and the executive responsibility for the running of the company's business. No one individual should have unfettered powers of decision.

Supporting Principle The chairman is responsible for leadership of the board, ensuring its effectiveness on all aspects of its role and setting its agenda. The chairman is also responsible for ensuring that the directors receive accurate, timely and clear information. The chairman should ensure effective communication with shareholders. The chairman should also facilitate the effective contribution of non-executive directors in particular and ensure constructive relations between executive and non-executive directors.

A.3 Board balance and independence

Main Principle The board should include a balance of executive and non-executive directors (and in particular independent non-executive directors) such that no individual or small group of individuals can dominate the board's decision taking.

Supporting Principles The board should not be so large as to be unwieldy. The board should be of sufficient size that the balance of skills and experience is appropriate for the requirements of the business and that changes to the board's composition can be managed without undue disruption. To ensure that power and information are not concentrated in one or two individuals, there should be a strong presence on the board of both executive and non-executive directors. The value of ensuring that committee membership is refreshed and that undue reliance is not placed on particular individuals should be taken into account in deciding chairmanship and membership of committees. No one other than the committee chairman and members is entitled to be present at a meeting of the nomination, audit or remuneration committee, but others may attend at the invitation of the committee.

A.4 Appointments to the Board

Main Principle There should be a formal, rigorous and transparent procedure for the appointment of new directors to the board.

Supporting Principles Appointments to the board should be made on merit and against objective criteria. Care should be taken to ensure that appointees have enough time available to devote to the job. This is particularly important in the case of chairmanships.

The board should satisfy itself that plans are in place for orderly succession for appointments to the board and to senior management, so as to maintain an appropriate balance of skills and experience within the company and on the board.

A.5 Information and professional development

Main Principle The board should be supplied in a timely manner with information in a form and of a quality appropriate to enable it to discharge its duties. All directors should receive induction on joining the board and should regularly update and refresh their skills and knowledge.

Supporting Principles The chairman is responsible for ensuring that the directors receive accurate, timely and clear information. Management has an obligation to provide such information but directors should seek clarification or amplification where necessary. The chairman should ensure that the directors continually update their skills and the knowledge and familiarity with the company required to fulfil their role both on the board and on board committees. The company should provide the necessary resources for developing and updating its directors' knowledge and capabilities. Under the direction of the chairman, the company secretary's responsibilities include ensuring good information flows within the board and its committees and between senior management and nonexecutive directors, as well as facilitating induction and assisting with professional development as required. The company secretary should be responsible for advising the board through the chairman on all governance matters.

A.6 Performance evaluation

Main Principle The board should undertake a formal and rigorous annual evaluation of its own performance and that of its committees and individual directors.

Supporting Principle Individual evaluation should aim to show whether each director continue to contribute effectively and to demonstrate commitment to the role (including commitment of time for board and committee meetings and any other duties). The chairman should act on the results of the performance evaluation by recognising the strengths and addressing the weaknesses of the board and, where appropriate, proposing new members be appointed to the board or seeking the resignation of directors.

A.7 Re-election

Main Principle All directors should be submitted for re-election at regular intervals, subject to continued satisfactory performance. The board should ensure planned and progressive refreshing of the **board.**

B. Remuneration

B.1 The Level and Make-up of Remuneration

Main Principles Levels of remuneration should be sufficient to attract, retain and motivate directors of the quality required to run the company successfully, but a company should avoid paying more than is necessary for this purpose. A significant proportion of executive directors' remuneration should be structured so as to link rewards to corporate and individual performance.

Supporting Principle The remuneration committee should judge where to position their company relative to other companies. But they should use such comparisons with caution, in view

of the risk of an upward ratchet of remuneration levels with no corresponding improvement in performance. They should also be sensitive to pay and employment conditions elsewhere in the group, especially when determining annual salary increases.

B.2 Procedure

Main Principle There should be a formal and transparent procedure for developing policy on executive remuneration and for fixing the remuneration packages of individual directors. No director should be involved in deciding his or her own remuneration.

Supporting Principles The remuneration committee should consult the chairman and/or chief executive about their proposals relating to the remuneration of other executive directors. The remuneration committee should also be responsible for appointing any consultants in respect of executive director remuneration. Where executive directors or senior management are involved in advising or supporting the remuneration committee, care should be taken to recognise and avoid conflicts of interest. The chairman of the board should ensure that the company maintains contact as required with its principal shareholders about remuneration in the same way as for other matters.

C. Accountability and Audit

C.1 Financial Reporting

Main Principle The board should present a balanced and understandable assessment of the company's position and prospects.

Supporting Principle The board's responsibility to present a balanced and understandable assessment extends to interim and other price-sensitive public reports and reports to regulators as well as to information required to be presented by statutory requirements.

C.2 Internal Control

Main Principle The board should maintain a sound system of internal control to safeguard shareholders' investment and the company's assets.

C.3 Audit Committee and Auditors

Main Principle The board should establish formal and transparent arrangements for considering how they should apply the financial reporting and internal control principles and for maintaining an appropriate relationship with the company's auditors.

D. Relations with Shareholders

D.1 Dialogue with Institutional Shareholders

Main Principle There should be a dialogue with shareholders based on the mutual understanding of objectives. The board as a whole has responsibility for ensuring that a satisfactory dialogue with shareholders takes place.

Supporting Principles Whilst recognising that most shareholder contact is with the chief executive and finance director, the chairman (and the senior independent director and other

directors as appropriate) should maintain sufficient contact with major shareholders to understand their issues and concerns. The board should keep in touch with shareholder opinion in whatever ways are most practical and efficient.

D.2 Constructive Use of the AGM
Main Principle The board should use the AGM to communicate with investors and to encourage their participation.

Section 2 Institutional Shareholders

E. Institutional Shareholders

E.1 Dialogue with companies
Main Principle Institutional shareholders should enter into a dialogue with companies based on the mutual understanding of objectives.

Supporting Principles Institutional shareholders should apply the principles set out in the Institutional Shareholders' Committee's "The Responsibilities of Institutional Shareholders and Agents – Statement of Principles" which should be reflected in fund manager contracts.

E.2 Evaluation of Governance Disclosures
Main Principle When evaluating companies' governance arrangements, particularly those relating to board structure and composition, institutional shareholders should give due weight to all relevant factors drawn to their attention.

Supporting Principle Institutional shareholders should consider carefully explanations given for departure from this Code and make reasoned judgements in each case. They should give an explanation to the company, in writing where appropriate, and be prepared to enter a dialogue if they do not accept the company's position. They should avoid a box-ticking approach to assessing a company's corporate governance. They should bear in mind in particular the size and complexity of the company and the nature of the risks and challenges it faces.

E.3 Shareholder Voting
Main Principle Institutional shareholders have a responsibility to make considered use of their votes.

Supporting Principles Institutional shareholders should take steps to ensure their voting intentions are being translated into practice. Institutional shareholders should, on request, make available to their clients information on the proportion of resolutions on which votes were cast and non-discretionary proxies lodged. Major shareholders should attend AGMs where appropriate and practicable. Companies and registrars should facilitate this.[87]

National Health Service (NHS) Returning to the UK, the NHS has a history of governance arrangements in this specialist part of the public sector. Like all large public service sectors, they have had their fair share of problems and unlike most service sectors each scandal is widely reported – since they can ultimately involve life and death issues. The NHS's May 2001 policies on corporate governance have an associated set of key criteria and cover the following areas:

Corporate Governance is the system by which an organisation is directed and controlled, at its most senior levels, in order to achieve its objectives and meet the necessary standards of accountability, probity and openness. Governance is therefore about achieving objectives, including value for money, and upholding public service values. For 2001/2002 and 2002/2003 the statement must identify what has been done and what is planned to achieve a risk-based approach to internal control across all the organisation's functions by the start of the financial year 2003/2004. The system of internal control in the NHS therefore, consists of financial, organisational and clinical components. Under HSC 1999/123 all NHS Trusts and Health Authorities will have a designated executive director who has overall responsibility for ensuring the implementation of Controls Assurance covering risk management and organisational controls, and for reporting to the board. Ultimately, the Chief Executives are accountable for having in place an effective system of risk management.

Criterion 1: The structure and constitution of the board, its committees and subcommittees, are in accordance with regulations and guidelines issued by the NHS Executive and are appropriate for the discharge of their duties.

Criterion 2: The conduct of the board reflects public service values and accords with the regulations and NHS Executive requirements for boards and committee behaviour.

Criterion 3: Standing orders, based on the example issued by the NHS Executive and updated to reflect current requirements, have been formally adopted by the board, and promulgated throughout the organisation.

Criterion 4: A schedule of decisions reserved by the board and a scheme of delegation have been formally adopted by the board, and are applied and observed consistently.

Criterion 5: Board responsibility for internal control is clearly defined and there are clear lines of accountability, reinforced by corporate and personal objectives, throughout the organisation for internal control including identifying and assessing risk. Board responsibility for internal control includes:

- understanding the risks, relating to objectives, strategies and policies (which the board should have set and approved), run by the organisation;
- setting acceptable levels for these risks and ensuring that senior management and other staff take steps necessary to identify, monitor and control these risks.

Criterion 6: The board of directors and senior management:

- promote high ethical and integrity standards;
- have established a culture within the organisation that emphasises and demonstrates to all levels of personnel the importance of internal control;
- all levels of staff understand their role in, and are fully engaged in, the internal control process.

Criterion 7: Senior management ensures that the internal and external risks that could adversely affect the achievement of the organisation's objectives are continuously and systematically identified and evaluated. This assessment covers all the various risks facing the organisation including operational risk, legal, financial, compliance risk and reputational risk.

Criterion 8: The board is systematically informed of all significant risks arising within the organisation and determines and appropriately records actions for their treatment.

Criterion 9: The board through senior management periodically ensures that all areas are in compliance with established policies and procedures.

Criterion 10: The overall effectiveness of the internal control in helping to achieve the organisation's objectives is continually monitored by the board and improvements made. Significant risks are monitored continually and separately evaluated as required.

Criterion 11: Sufficient and appropriate records are kept and archived of all major control systems (e.g. records of policies and procedures, management review, budgetary control, performance indicators, information processing, physical controls such as checking inventory or cash to records, segregation of duties, signing, countersigning and double checking.

Criterion 12: Effective channels of communication are established to ensure that all staff, and stakeholders where relevant, are fully aware of policies and procedures affecting their duties and responsibilities and that other relevant information reaches the appropriate personnel.

Criterion 13: Effective channels of communication exist to ensure that all staff can communicate upwards, downwards and across about matter relevant to their work.

Criterion 14: The organisation communicates effectively with its external stakeholders.

Criterion 15: The board at least annually conducts a review of the effectiveness of the organisation's systems of internal control and reports in the annual report that it has done so.

Criterion 16: All employees, including management and the board, should be provided, where appropriate, with adequate information, instruction and training on corporate governance and internal control and risk management issues.

Criterion 17: Key indicators capable of showing improvements in corporate governance including internal controls are used at appropriate levels of the organisation and the usefulness and efficacy of the indicators is reviewed regularly.

Criterion 18: The audit committee reports formally to the board on the measures it has taken to verify that there is a systematic and comprehensive review of corporate governance including the effectiveness of internal control, and the results of such reviews.

Criterion 19: There is an adequately resourced, trained and competent internal audit function whose role includes providing the audit committee with an independent and objective opinion on the effectiveness of the organisation's systems of internal control.

The NHS has gone on to develop what they call an integrated governance process, which is described below:

Integrated Governance

Integrated Governance is defined as: 'Systems, processes and behaviours by which trusts lead, direct and control their functions in order to achieve organisational objectives, safety and quality of service and in which they relate to patients and carers, the wider community and partner organisations'

Part 2: How TO DO IT

Assurance and controls – Meeting Board responsibilities All Boards need systems of reporting and monitoring that keep them informed of the progress of their objectives, the

development and assessment of risks and issues that threaten the achievement of the objectives. Implementing the Assurance Framework and the Department of Health's Standards for Better Health will enable the Board to be sure that it is in full control of its agenda.

The Assurance Framework The following extracts from 'Building the Assurance Framework – A Practical Guide for NHS Boards' (DH, 2003) clearly indicate what the Board must do when developing an Assurance Framework:

More than ever before, as the NHS embraces a culture of decentralisation, increasing local autonomy and local accountability, Boards need to be confident that their systems, policies and people are operating in a way that is effective in driving the delivery of objectives by focusing on identifying, prioritising and minimising risk. In support of that challenge, in July 2002 the Department of Health issues "Assurance: The Board Agenda" which set out the principles for an Assurance Framework to give Boards the confidence they need. This has now been further developed in "Building the Assurance Framework".

The requirement for all NHS Chief Executive Officers to sign a Statement on Internal Control (SIC) as part of the statutory accounts and annual report, heightens the need for Boards to be able to demonstrate that they have been properly informed about the totality of their risks, both clinical and non-clinical. To do this they need to be able to provide evidence that they have systematically identified their objectives and managed the principal risks to achieving them. The Assurance Framework fulfils this purpose. 'There has been considerable interest in receiving additional direction and advice on building an Assurance Framework, and on how to bring together the existing fragmented risk management activity systematically and make sure that the process is efficient, highly focused and adds real benefits to the organisation. This section therefore describes how to construct an Assurance Framework, supported by worked examples. It also clarifies the relationship with performance management arrangements, clinical governance reporting and other sources of assurance. This does not introduce any new requirements on NHS organisations, but tries to provide practical assistance and clarity about what is currently required.' in summary:

- Establish principal objectives (strategic and directorate).
- Identify the principal risks that may threaten the achievement of these objectives – but ensure that there is the opportunity to recognise critical risks outside key objectives.
- Identify and evaluate the design of key controls intended to manage these principal risks, underpinned by core controls assurance standards.
- Set out the arrangements for obtaining assurance on the effectiveness of key controls across all areas of principal risk.
- Evaluate the assurance across all areas of principal risk.
- Identify positive assurances and areas where there are gaps in controls and/or assurances.
- Put in place plans to take corrective action where gaps have been identified in relation to principal risks.
- Maintain dynamic risk management arrangements including, crucially, a well founded risk register.

The Assurance Framework provides organisations with a simple but comprehensive method for the effective and focused management of the principal risks to meeting their objectives. It also provides a structure for the evidence to support the SIC. This simplifies Board reporting and the prioritisation of action plans which, in turn, allow for more effective performance management.

Internal Audit

Internal auditors provide an opinion about the Assurance Framework to the client organisation at the year-end. This is in two distinct parts. The first is an opinion on the adequacy of the Assurance Framework itself; the second is to provide assurances on the management of those risks identified within the Assurance Framework, where the internal auditors have carried out review work during the year. This opinion is used by the Board to inform the SIC and by the Strategic Health Authority as part of its performance management role. It is also likely that Internal Audit will play a key role in supporting Trust assurances to the Healthcare Commission on compliance with standards.

External Audit

External auditors are required to review the SIC as part of their annual audit of the financial statements. The review considers whether the SIC has been prepared in accordance with the Department of Health's requirements, and whether there are any inconsistencies between the disclosures in the SIC and information the auditors are aware of from their work on the financial statements and any other work. To inform their review, auditors will consider the governance arrangements in place at NHS bodies and will place reliance on the Assurance Framework as the key piece of evidence in support of the SIC.[88]

Central government The Treasury is responsible for setting standards across government relating to accounting, internal audit and accountability. They have tracked developments in the private sector and spent some time considering how the corporate governance codes can be adapted (rather than adopted) to sit with government organizations. The responsibility for governance is vested in the designated accounting officer for the organization in question with the added complication of ministerial oversight of the service provided. The accounting officer is appointed by the Treasury or designated by a department to be accountable for the operations of an organization and the preparation of its accounts. The accounting officer is normally the chief executive of the body. Some commentators have suggested that the term corporate governance is not appropriate for government organizations, since 'corporate' is associated with commercial enterprises and 'governance' is primarily what government is all about. Notwithstanding these differences, the Treasury view is that aspirations to adopt best practice in managing corporate Britain has value in all sectors of society. Government sector organizations have adhered to the requirement to prepare a statement on internal financial control for some years since 1998/1999, and as mentioned earlier, this is really an extension of the external audit work supplemented by any internal audit involvement in financial systems. The breakthrough that parallels similar developments in the private sector came with Treasury guidance DAO 13/00, which applied for accounts beginning on or after 1 January 2001 where the accounting officer has to prepare a statement of internal control (SIC) to accompany the annual report and accounts. Each organization had three years to become fully compliant with the guidance, so that they might report fully by 2003/2004. The SIC should explain the nature of control, and any material changes in control, exercised through the whole of the accounting period. The accounting officer should, as part of their annual review of the SIC, ensure that their internal audit provision is adequately resourced to deliver a service in accordance with the standards in the *Government Internal Audit Manual*. The guidance includes an Annex A2 that gives examples of such statements of internal

control depending on how far the underlying structures and processes have been developed. Extracts from Annex A2 follow:

> As Accounting Officer, I have responsibility for maintaining a sound system of internal control that supports the achievement of departmental policies, aims and objectives, set by the department's Ministers, whilst safeguarding the public funds and departmental assets for which I am personally responsible, in accordance with the responsibilities assigned to me in Government Accounting. The system of internal control is designed to manage rather than eliminate the risk of failure to achieve policies, aims and objectives; it can therefore only provide reasonable and not absolute assurance of effectiveness. The system of internal control is based on an ongoing process designed to identify the principal risks to the achievement of departmental policies, aims and objectives, to evaluate the nature and extent of those risks and to manage them efficiently, effectively and economically. This process has been in place for the year ended 31 March 200x and up to the date of approval of the annual report and accounts and accords with Treasury guidance. As Accounting Officer, I also have responsibility for reviewing the effectiveness of the system of internal control. The department has established the following processes:
>
> - a management board which meets monthly to consider the plans and strategic direction of the department . . . ;
> - periodic reports from the chairman of the audit committee, to the board, concerning internal control;
> - regular reports from internal audit, to standards defined in the GIAM, which include the Head of Internal Audit's independent opinion on the adequacy and effectiveness of the department's system of internal control together with recommendations for improvement;
> - regular reports from managers on the steps they are taking to manage risks in their areas of responsibility including progress reports on key projects;
> - a regular programme of facilitated workshops to identify and keep up to date the record of risks facing the organisation;
> - a programme of risk awareness training;
> - implementation of a robust prioritisation methodology based on risk ranking and cost-benefit analysis;
> - establishment of key performance and risk indicators;
> - maintenance of an organisation-wide risk register;
> - reports from the chief executive on the department's agencies on internal control activities;
> - reports on compliance with the principal recommendations in the Cabinet Office report on Successful IT: Modernising Government in Action.
>
> My review of the effectiveness of the system of internal control is informed by the work of the internal auditors and the executive managers within the department who have responsibility for the development and maintenance of the internal control framework, and comments made by the external auditors in their management letter and reports.

The Treasury guidance focuses heavily on risk management across each organization and is used in conjunction with an associated guide to strategic risk management (known as The Orange Book). Again, the implementation of a reliable system of risk management enables the accounting officer to give a robust position on the internal controls in place to manage areas of high risk. A further aspect of managing risk is to ensure that any risks that impact the public, have to be communicated carefully and with due regard to the need to balance the information provided. Moreover, moving controls away from finance to the business operations brings people into contact with control review practices who have never had this type of involvement before. Hence

the heavy emphasis on training and awareness. The 2005 Corporate governance code for central government departments develops some of the themes that are now high on the governance agenda:

> The Accounting Officer is also responsible to Parliament, in respect of the deployment of public money, to consider value for money from the point of view of the wider Exchequer. At the request of the departmental Accounting Officer, other senior officials in the department may be appointed as Additional Accounting Officers for certain accounts, Requests for Resources (RfRs), or distinct parts of an Estimate. It is best practice for at least one Additional Accounting Officer to be appointed in larger departments. However, the departmental Accounting Officer retains overall responsibility to Parliament for ensuring a high standard of financial management in the department as a whole.
>
> **PRINCIPLES 1.** The minister in charge of the department is responsible and answerable to Parliament for the exercise of the powers on which the administration of that department depends. He or she has a duty to Parliament to account, and to be held to account, for all the policies, decisions and actions of the department including its executive agencies. 1B. Under the minister, the head of the department, as its Accounting Officer, is also personally responsible and accountable to Parliament for the management and organisation of the department, including the use of public money and the stewardship of its assets.
>
> **PRINCIPLE 2.** Each department should be managed by an effective board which, within the strategic framework set by the minister (or, in the case of a non-ministerial department, by legislation), supports the head of the department by advising ministers and taking ownership of the department's performance.
>
> **PRINCIPLE 3.** The board's membership should have a balance of skills and experience appropriate to directing the business of the department.
>
> **PRINCIPLE 4.** The board should include independent non-executive members to ensure that executive members are supported and constructively challenged in their role.
>
> **PRINCIPLE 5.** The board should ensure that effective arrangements are in place to provide assurance on risk management, governance and internal control. In this respect, the board should be independently advised by:
>
> - an audit committee chaired by an independent non-executive member;
> - an internal audit service operating in accordance with Government Internal Audit Standards.
>
> **PRINCIPLE 6.** Where part of the business of the department is conducted with and through arm's length bodies (ALBs), the department's board should ensure that there are robust governance arrangements with each ALB board, setting out the terms of their relationship, in order to promote high performance and safeguard propriety and regularity.[89]

Californian Public Employees' Retirement System (CalPERS)

The US experience is much the same as the UK's even though their corporate accountability structures and Securities and Exchange Commission (SEC) regulations differ in some respects. The CalPERS represent US investors and are key stakeholders for corporate America. As such, they are concerned with the proper running of large corporations and the governance processes they adopt and report on. CalPERS have developed a set of US Corporate Governance Principles (Core Corporate Governance Principles) summarized as follows:

1. A substantial majority of the board consists of directors who are independent.
2. Independent directors meet periodically (at least once a year) without the CEO or other non-independent directors.
3. When the chair of the board also serves as the company's CEO, the board designates formally or informally an independent director who acts in a lead capacity to coordinate the independent directors.
4. Certain board committees consist entirely of independent directors including:
   - audit
   - director nomination
   - board evaluation and governance
   - CEO evaluation and management compensation
   - compliance and ethics.
5. No director may also serve as a consultant or service provider to the company.
6. Director compensation is a combination of cash and stock in the company. The stock component is a significant portion of the compensation.

The theme for this code is the independence of directors and the use of committees to reinforce the oversight role. This is an important balancing mechanism where the huge power vested in the CEO is countered by the presence of independent persons who are able to ask tough questions where appropriate. Note that many of these types of codes are somewhat sidelined by developments in SEC rules that appeared towards the end of 2002. More recently, CalPERS has developed a set of Global Principles that are broken down into four areas – core, domestic, international, and emerging markets. CalPERS believes that the criteria contained in the Core Principles may be adopted by companies across all markets which are summarized below:

> There are many features that are important consideration in the continuing evolution of corporate governance best practices. However, the underlying tenet for CalPERS Core Principles of Accountable Corporate Governance is that fully accountable corporate governance structures produce, over the long term, the best returns to shareowners. CalPERS believes the following Core Principles should be adopted by companies in all markets – from developed to emerging – in order to establish the foundation for achieving longterm sustainable investment returns through accountable corporate governance structures.

1. Optimizing Shareowner Return: Corporate governance practices should focus the board's attention on optimizing the company's operating performance, profitability and returns to shareowners.
2. Accountability: Directors should be accountable to shareowners and management accountable to directors. To ensure this accountability, directors must be accessible to shareowner inquiry concerning their key decisions affecting the company's strategic direction.
3. Transparency: Operating, financial, and governance information about companies must be readily transparent to permit accurate market comparisons; this includes disclosure and transparency of objective globally accepted minimum accounting standards, such as the International Financial Reporting Standards ("IFRS").
4. One-share/One-vote: All investors must be treated equitably and upon the principle of one-share/one-vote.
5. Proxy Materials: Proxy materials should be written in a manner designed to provide shareowners with the information necessary to make informed voting decisions. Similarly, proxy materials should be distributed in a manner designed to encourage shareowner participation. All shareowner votes, whether cast in person or by proxy, should be formally counted with vote outcomes formally announced.

6. Code of Best Practices: Each capital market in which shares are issued and traded should adopt its own Code of Best Practices to promote transparency of information, prevention of harmful labor practices, investor protection, and corporate social responsibility. Where such a code is adopted, companies should disclose to their shareowners whether they are in compliance.
7. Long-term Vision: Corporate directors and management should have a long-term strategic vision that, at its core, emphasizes sustained shareowner value. In turn, despite differing investment strategies and tactics, shareowners should encourage corporate management to resist shortterm behavior by supporting and rewarding long-term superior returns.
8. Access to Director Nominations: Shareowners should have effective access to the director nomination process.[90]

Canada – the Dey Report

The Dey report was published in 1994 which set the framework for corporate governance in Canada. An updated view appeared in the November 2001 report, Beyond Compliance: Building a Governance Culture, by the Canadian Institute of Chartered Accountants, Canadian Venture Exchange, Toronto Stock Exchange. This report argued that there are several key issues that go beyond compliance and are fundamental to building a healthy governance culture:

1. measures that can be taken to strengthen the capacity of the board to engage in a mature and constructive relationship with management – one that is grounded in a mutual understanding of respective roles and the ability of the board to act independently in fulfilling its responsibilities;
2. the critical role that the board must play in choosing the CEO . . . ;
3. particular issues that independent directors must face in corporations that have significant shareholders.

Selected extracts follow:

- The objective of corporate governance is to promote strong, viable and competitive corporations. Boards of directors are stewards of the corporation's assets and their behaviour should be focused on adding value to those assets by working with management to build a successful corporation and enhance shareholder value. (page 10)
- Not only is disclosure preferable to regulation as a tool to change behaviour, it is also appropriate. The evolution of capital markets has clearly shown that disclosure instils discipline and increases efficiency. With regards to corporate governance, we see two important benefits that can assist boards that are looking for ways to become more effective. Second, a requirement to disclose against guidelines ways to become more effective by forcing boards to focus explicitly on their roles and responsibilities and how they are being discharged. (page 13)
- Recommendation 2 (2) Boards should actively look beyond traditional sources in seeking men and women with the right mix of experience and competencies. Diversity of background and experience can add value to boardroom deliberations . . . (page 18)
- If boards are to add value, they must involve themselves actively and regularly in the function of strategic planning and risk management. We believe that these functions need to be closely integrated: strategic planning should be based upon an identification of opportunities and the full range of business risks that will condition which of those opportunities are most worth pursuing. Strategic planning is an ongoing process that must be responsive to changes in

the external environment and the internal developments. Flexibility and responsiveness are critical. In this sense, strategic planning is a much broader concept than developing a business plan and should include assessments of opportunities and risks across a range of areas . . . (page 24)

- They (effective boards) will oversee the processes that management has in place to identify business opportunities and risks. They will consider the extent and type of risk that is acceptable for the company to bear. They will monitor management's systems and processes for managing the broad range of business risk. And most important, on an ongoing basis, they will review with management how the strategic environment is changing, what key business risks and opportunities are appearing, how they are being managed and what, if any, modifications in strategic direction should be adopted. (page 24)

The Dey report, as with all governance material, the guidance is being continually updated to reflect current developments.

The King Report

A major document from South Africa appeared in March 2002 and brought Africa into the corporate governance debate. The chairperson of the King Committee on Corporate Governance, Mervyne E. King, SC, prepared the report with support from the IoD (Centre for Directorship and Corporate Governance). Updating the 1994 King report, the Task Team also considered international best practice in recognition of what they termed 'our borderless world of the information.' The King report is remarkable because it is built on the wealth of knowledge and material that has been developed over the years since Cadbury was first reported. The Executive Summary lists the key areas and, because it is so inclusive in its coverage of corporate governance issues, the reader will reap dividends for working through the following provisions selected from the code:

EXECUTIVE SUMMARY:

5.1 One is liable to render an account when one is accountable and one is liable to be called to account when one is responsible, boards need to identify their stakeholders and agree policies on how to manage these relationships but cannot be accountable to everyone = accountable to no one.

5.2 Influences and stakeholders – regulators, industry and market standards, reputation, investigative media, customers, suppliers, consumers, employees, investors, communities, political opinion, ethical pressure groups = contractual and non contractual.

6. Inclusive long term approach is where the company defines values and communicates these to its identified stakeholders – for a mutually beneficial relationship.

7.1 Emerging economies are driven by entrepreneurs who take business risks.

7.2 Key challenge – performance and conformance.

8. Three corporate sins – sloth, greed, and fear. The protection against greed could create sloth and fear.

13. Blurring of organisational barriers due to e-business impacts on internal controls.

14. Physically a company may move around the world but must still live up to its reporting responsibilities – tax, labour and regulation havens.

15. With the global market companies must compete to be the destination of choice.

16. Arthur Levitt former chairman of the US SEC said . . . If a country does not have a reputation for strong corporate governance practices, capital will flow elsewhere . . . It serves us well to remember that no market has a divine right to investors' capital.

17. There is a move from the single to the triple bottom line, which embraces the economic, environmental and social (stakeholders) aspects of a company's activities.

17.3 The company is a separate persona in law and therefore has obligations to others as well as shareholders. Shareholders only have a right to vote and a right to dividends.

18. Seven characteristics of CG:
    1. Discipline – correct and proper behaviour.
    2. Transparency – true picture of what is happening.
    3. Independence – no undue influences.
    4. Accountability – actions of the board may be assessed.
    5. Responsibility – to all stakeholders.
    6. Fairness – rights of various groups respected.
    7. Social responsibility – good corporate citizen.

24. 19th Century entrepreneurs
    20th Century management
    21st Century governance

26. Some companies have appointed corporate reputation officers to manage how the company is seen by outsiders. Non financial performance indicators include – customer perceptions, morale, innovation, training, relations with stakeholder, management credibility, internal audit, management information systems, risk management, productivity, and service standards.

The King report is regularly updated and King III came out in 2009 (The King Code of Governance For South Africa, published by the IoD in Southern Africa) making reference to the credit crunch and the need to strengthen corporate governance on the back of the 2007–2009 financial crisis. King III also made reference to the 'light touch' approach to regulation in contrast to the more robust approach used in the US as they used Sarbanes–Oxley to help recover from the WorldCom–Enron scandals. King III is based on leadership, sustainability and corporate citizenship and recommended several changes to support corporate citizenship and better business sustainability through improved governance arrangements in South Africa. The new stance seeks to better integrate social, environmental and economic issues and suggests what they call an 'enlightened shareholder' model as well as the 'stakeholder inclusive' model of corporate governance where the informed investor assesses, among other things, the quality of the company's risk management. One interesting topic that is covered relates to risk-based internal auditing where Mervyn E King discusses the move away from a compliance–based approach. This contrasts with many other governance codes, which only pay a passing interest to the internal audit role. The nine chapters of King III contain key principles of governance and explain how to apply these principles through various best practice recommendations. The report says that entities should apply the principles in the Code and consider the best practice recommendations in the Report and make a positive statement about how the principles have been applied or have not been applied and the new version, updating King II, is effective from Summer 2010.

Australia

As with other developed economies, the Australians have derived material concerning the way companies and the public sector should be governed. The Australian Stock Exchange Rule 3C(3)(j) requires Australian companies to provide a statement of the main corporate governance practices that have been in place during the reporting period. A presentation by Pat Barrett (Auditor General for Australia on 'What's New in Corporate Governance at the Certified Public

Accountant (CPA) Australia Annual Congress', Adelaide, 17 November 2000, www.anao.gov.au) contains many interesting points concerning the concept of accountability and governance in Australia, including the need to place substance over technical form and to ensure suitable structures and culture are in place:

- The emphasis is now very much on personal responsibility starting with the CEO. Greater management flexibility and commensurate increases in personal accountability and, arguably, in the degree of risks required to be handled by agency management are the hallmarks of the ongoing public sector reform movement.
- As well, there is some need for more dialogue between business, government and the community. Indeed, some are now advocating the embrace by business of the 'triple bottom line' reporting with a focus on financial as well as environmental and social accountability . . .
- The emerging less regulatory environment is characterised by efforts at 'deregulation', simplification, streamlining, coupled with efforts by government to reinforce the essential 'contract' between consumers (or clients) and the providers of goods and services, whether in the private or public sector.
- In short information communications technology is, increasingly, both determining the nature and structures of governance and corporate governance as well as being used by such frameworks to achieve required results, deal positively with risks, observe legislation and regulating requirements and be responsive and accountable to stakeholders.
- CG is largely about organisational and management performance. Simply put, CG is about how an organisation is managed, its corporate and other structures, its culture, its policies and the ways in which it deals with its various stakeholders. It is concerned with structures and processes for decision-making and with the controls and behaviour that support effective accountability for performance outcomes/results. Key components of CG in both the private and public sectors are business planning, risk management, performance monitoring and accountability.
- Concern has been expressed, in both the public and private sectors, that there has been more emphasis on the form rather than the substance of good CG. The challenge is not simply to ensure that all the elements of CG are effectively in place but that its purposes are fully understood and integrated as a coherent and comprehensive organisational strategy focused on being accountable for agency and entity conduct and results . . . conformance v performance.

The Australian *ASX Corporate Governance Council* has developed a set of Corporate Governance Principle and Recommendations that cover some important areas and extracts from the foreword are reproduced below:

> This document cannot be the final word. It is offered as guidance and will be reviewed again. Nor is it the only word. Good corporate governance practice is not restricted to adopting the Council's Recommendations. The arrangements of many entities differ from the Recommendations but amount equally to good practice. What matters is disclosing those arrangements and explaining the governance practices considered appropriate to an individual company's circumstance. We are all – the Council, ASX and Australian market participants generally – in the business of preserving stakeholder confidence. That is the thread that runs through each of the Principles and Recommendations contained in this document. The wording may change, as necessary, from time to time, but that underlining theme will remain.[91]

The Australian code also contains a number of key principles and each one is supported by a set of recommendations. The corporate governance principles are noted below:

Principle 1 – Lay solid foundations for management and oversight

Companies should establish and disclose the respective roles and responsibilities of board and management.

Principle 2 – Structure the board to add value

Companies should have a board of an effective composition, size and commitment to adequately discharge its responsibilities and duties.

Principle 3 – Promote ethical and responsible decision-making Companies should actively promote ethical and responsible decision-making.

Principle 4 – Safeguard integrity in financial reporting

Companies should have a structure to independently verify and safeguard the integrity of their financial reporting.

Principle 5 – Make timely and balanced disclosure

Companies should promote timely and balanced disclosure of all material matters concerning the company.

Principle 6 – Respect the rights of shareholders

Companies should respect the rights of shareholders and facilitate the effective exercise of those rights.

Principle 7 – Recognise and manage risk

Companies should establish a sound system of risk oversight and management and internal control.

Principle 8 – Remunerate fairly and responsibly

Companies should ensure that the level and composition of remuneration is sufficient and reasonable and that its relationship to performance is clear.[91]

The OECD

The OECD has summed up many of the global principles of good corporate governance, and extracts are shown below:

I. Ensuring the Basis for an Effective Corporate Governance Framework

The corporate governance framework should promote transparent and efficient markets, be consistent with the rule of law and clearly articulate the division of responsibilities among different supervisory, regulatory and enforcement authorities.

II. The Rights of Shareholders and

Key Ownership Functions

The corporate governance framework should protect and facilitate the exercise of shareholders' rights.

III. The Equitable Treatment of Shareholders

The corporate governance framework should ensure the equitable treatment of all shareholders, including minority and foreign shareholders. All shareholders should have the opportunity to obtain effective redress for violation of their rights.

IV. The Role of Stakeholders in Corporate Governance

The corporate governance framework should recognise the rights of stakeholders established by law or through mutual agreements and encourage active co-operation between corporations and stakeholders in creating wealth, jobs, and the sustainability of financially sound enterprises.

V. Disclosure and Transparency

The corporate governance framework should ensure that timely and accurate disclosure is made on all material matters regarding the corporation, including the financial situation, performance, ownership, and governance of the company.

VI. The Responsibilities of the Board

The corporate governance framework should ensure the strategic guidance of the company, the effective monitoring of management by the board, and the board's accountability to the company and the shareholders.[92]

The Institute of Internal Auditors

There are many other codes and guides from almost every country that has a developed market for shares and securities. The IIA has a leading role in considering issues relating to corporate governance and assessing how internal auditors can contribute to the growth in this evolution. The IIA.Inc. have prepared Professional Guidance that endorses the work of Kennesaw State University – Corporate Governance Center, involving over 20 professors from several universities who developed the following principles of corporate governance:

1. **Interaction** – Sound governance requires effective interaction among the board, management, the external auditor, and the internal auditor.
2. **Board Purpose** – The board of directors should understand that its purpose is to protect the interests of the corporation's stockholders, while considering the interests of other stakeholders (e.g., creditors, employees, etc.).
3. **Board Responsibilities** – The board's major areas of responsibility should be monitoring the CEO, overseeing the corporation's strategy, and monitoring risks and the corporation's control system. Directors should employ healthy skepticism in meeting these responsibilities.
4. **Independence** – The major stock exchanges should define an 'independent' director as one who has no professional or personal ties (either current or former) to the corporation or its management other than service as a director. The vast majority of the directors should be independent in both fact and appearance so as to promote arms-length oversight.
5. **Expertise** – The directors should possess relevant industry, company, functional area, and governance expertise. The directors should reflect a mix of backgrounds and perspectives. All directors should receive detailed orientation and continuing education to assure they achieve and maintain the necessary level of expertise.
6. **Meetings and Information** – The board should meet frequently for extended periods of time and should have access to the information and personnel it needs to perform its duties.
7. **Leadership** – The roles of Board Chair and CEO should be separate.
8. **Disclosure** – Proxy statements and other board communications should reflect board activities and transactions (e.g., insider trades) in a transparent and timely manner.

9. **Committees** – The nominating, compensation, and audit committees of the board should be composed only of independent directors.
10. **Internal Audit** – All public companies should maintain an effective, full-time internal audit function that reports directly to the audit committee.
11. **Reporting Model** – The current GAAP financial reporting model is becoming increasingly less appropriate for U.S. public companies. The industrial-age model currently used should be replaced or enhanced so that tangible and intangible resources, risks, and performance of information-age companies can be effectively and efficiently communicated to financial statement users. The new model should be developed and implemented as soon as possible.
12. **Philosophy and Culture** – Financial statements and supporting disclosures should reflect economic substance and should be prepared with the goal of maximum informativeness and transparency. A legalistic view of accounting and auditing (e.g., 'can we get away with recording it this way?') is not appropriate. Management integrity and a strong control environment are critical to reliable financial reporting.
13. **Audit Committees** – The audit committee of the board of directors should be composed of independent directors with financial, auditing, company, and industry expertise. These members must have the will, authority, and resources to provide diligent oversight of the financial reporting process. The board should consider the risks of audit committee member stock/stock option holdings and should set audit committee member compensation at an appropriate level given the expanded duties and risks faced by audit committee members. The audit committee should select the external auditor, evaluate external and internal auditor performance, and approve the audit fee.
14. **Fraud** – Corporate management should face strict criminal penalties in fraudulent financial reporting cases. The Securities and Exchange Commission should be given the resources it needs to effectively combat financial statement fraud. The board, management, and auditors all should perform fraud risk assessments.
15. **Audit Firms** – Audit firms should focus primarily on providing high-quality audit and assurance services and should perform no consulting for audit clients. Audit firm personnel should be selected, evaluated, compensated, and promoted primarily based on technical competence, not on their ability to generate new business. Audit fees should reflect engagements' scope of work and risk.
16. **External Auditing Profession** – Auditors should view public accounting as a noble profession focused on the public interest, not as a competitive business. The profession should carefully consider expanding audit reports beyond the current 'clean' versus modified dichotomy so as to enhance communication to financial report users.
17. **Analysts** – Analysts should not be compensated (directly or indirectly) based on the investment banking activities of their firms. Analysts should not hold stock in the companies they follow, and they should disclose any business relationships between the companies they follow and their firms.[93]

Several years ago, the IIA.UK&Ireland issued their recommendations for corporate governance reforms in a paper entitled 'A New Agenda for Corporate Governance Reform' in the fallout from Enron and WorldCom. Neil Baker has summarized this paper:

1. A stronger code of corporate governance for UK listed companies so that a uniform set of principles is enforced, as opposed to the current system of 'comply or explain'.
2. Enforced rotation of the external audit partners and audit managers every seven years, preferably every five years.
3. Disclosures made in the annual report of all non-audit work carried out by the external auditor.

4. Non-executive directors should not be former officers or directors of the business.
5. The audit committee should be composed of at least three members, all of whom should be non-executive directors, including the committee chair.
6. Boards should be required to disclose an assessment of the effectiveness of their internal controls.
7. All publicly held companies should establish and maintain an independent, adequately resourced and competently staffed internal audit function.[94]

2.5 Putting Governance into Practice

As a start we need to consider the ways corporate governance can be made to work in practice. Andrew Chambers' book on corporate governance provides a simple list of what he calls the ten 'principia' of effective corporate governance as follows:

1. Stakeholder control of the business.
2. Maximum and reliable public reporting.
3. Avoidance of excessive power at the top of the business.
4. A balanced board composition.
5. A strong involved board of directors.
6. A strong, independent element on the board.
7. Effective monitoring of management by the board.
8. Competence and commitment.
9. Risk assessment and control.
10. A strong audit presence.[95]

This represents a good starting place for considering some of the published positions on corporate governance. We follow this with several examples of extracts from disclosure statements from various large companies.

The Tipping Point For Board Oversight Of IT

By Dan Swanson, *Compliance Week Columnist*

Traditionally, and properly, a company's board of directors has focused on governing the organization; that is, the board ensures that the right CEO is in place, that the right business strategies have been developed, that performance is reported regularly and trending properly, and that the right questions are being asked of management. The board's agenda is truly endless, and it is absolutely critical that the board not micromanage the CEO, attempt to ''manage'' the organization, or have items on its agenda that are not focused on the long-term success of the organization. The board should revisit its mandate periodically, reconfirming its roles and responsibilities. We need to pose, the question of what the board's oversight role is regarding information technology. There is no one right answer to this question, it can even be said the short answer is, ''It depends.'' Indeed, many believe it is not the purview of the board to discuss IT strategy; the board is there to provide oversight to management's efforts, and since IT is only a ''tool'' in achieving those business strategies, in general it should not be on the board's agenda. At the other end of the spectrum there are those who maintain that IT is the business for most organizations today, and that as IT goes, so goes the company. Therefore, the board needs to be informed and participate in discussions about IT investments, including the organization's IT strategies, plans, and processes.

Finally, there are others who believe IT or IT security will be the source of our next Enron-style corporate malfeasance, so the board needs to be much more active with IT and IT security efforts.

Revisit, Review, Reconsider

My recommendation is that the board should review and define its oversight role regarding IT. That is, the board should understand how important the IT activities are to the organization's implementation of business strategies, what IT initiatives are critical to the organization's success, what the strengths and weaknesses of the IT management team are, and what, if any, changes should be instituted regarding the board oversight of IT.

A basic focus of the board is ensuring corporate viability, and protecting and increasing shareholder value. If IT is so critical today to the long-term success of the company, then the board should provide oversight of IT. The board should not get involved in day-to-day management, but it must maintain active oversight. IT is a key contributor to the organization's results, including the always visible financial reporting and disclosure effort – and we all know what happens with incorrect financial reporting.

A fundamental question for each organization to investigate and answer is whether board oversight of IT is a ''missing piece to the puzzle'' in its board governance or if it is a non-issue for that organization. While the answer is most likely somewhere in the middle of these two extremes, it is up to the board to decide its mandate including its roles, responsibilities, and various oversight processes. The industry involved can be a factor regarding the degree of oversight needed. Obviously an IT company and others in the technology sector should consider having a few board directors with IT expertise. Such companies probably need greater board oversight over IT strategy and investments than others, with some even having a board-level technology committee. There are actually few industries today where IT governance is not significant, although the financial, health, and technology sectors certainly require more oversight than others.

Defining The Board's IT Oversight Role

And why is board oversight of IT so important today? Consider:

1. The growing extent that corporate productivity is now related to ''intellectual capital.'' With IT so essential to creating organizational value, boards need to understand IT better. That isn't captured through monitoring other, more traditional areas.
2. Productivity growth statistics, and estimates of how much of that growth is caused by smart use of IT. Everyone is in a competitive business, and IT can give companies a competitive advantage.

Just because the board has not taken an active role in IT in the past or put IT on the board agenda very frequently, that does not mean there isn't a place for the board regarding IT. It's always better to decide the board's role going forward than to have

it dictated by the next Enron that occurs. I also believe that periodically revisiting the board's mandate and its various committees' terms of reference is a productive activity in this never-ending effort to improve governance and organizational performance. And at the end of the day, isn't that what it is all about? The board's governance of the company as it relates to IT will depend on the nature of the organization and also of risks, both strategic and tactical. The board's involvement is likely to vary over time. The board's involvement in IT should be driven in the same way as it gets involved in marketing, personnel, legal, and other departments – in that there is no ''automatic'' involvement in IT. You must decide your board's involvement and then act to achieve it.

Governance is fundamentally about identifying and managing strategic risk to the organization, whether that's the risk of the CEO turning out to be a crook, or the business strategy itself being flawed. If the organization doesn't use IT, there's obviously no risk. If the organization has enterprise-level investment in (and dependence on) information and IT, then there is risk. It is the scale of the risk that determines whether or not board oversight is necessary. Small risk, who cares? Big risk, think betting the farm on a technology project, then the board had better oversee it. We don't need to oversee day-to-day management of IT (other than perhaps agreeing the criteria for recruiting the CIO), but we might think that there are half a dozen key performance indicators that we want to see on a regular basis that tells us how well this part of the business is being managed. There is no hard and fast rule beyond managing risk; which board wants to be on duty when an IT project leads to the company going down? Crying, ''We left it to management!'' will be just another way of saying, ''Please sue us, because we took our fees but we just weren't paying attention.''

In my view, board oversight of IT is essential. For an ever-wider range of industries, IT is too important to be left to technologists alone. That said, the board must limit the nature of its involvement to strategic issues. The board should not be involved in where to draw the line in each case, but it should be sure that management is aware of the need to weigh the pros and cons and make an explicit decision in each case. The decision is basically one to be made on business grounds with a proper understanding of the potential, the risks and the constraints of available technology. Too often the business dimension will not even be considered if these decisions are left to technology experts alone. Further significant insights are provided in the resources identified below, has your organization reached its tipping point?

Reprinted from Compliance Week. This article was originally published in Compliance Week. Reproduced by permission of Compliance Week. All rights reserved.

Governance and Policy Disclosures

GlaxoSmithKline

Governance and policy

Board committees:

- The Audit Committee reviews the financial and internal reporting process, the systems of internal control and management of risks and the external and internal audit processes. The Committee consists entirely of NEDs. It meets four times a year with the CEO, CFO, the

General Council, and the head of internal audit and corporate compliance with the external auditors in attendance.
- The Finance Committee reviews and approves the major financial and securities transactions of the company as well as dividends, results announcements and the business of the Annual General Meeting . . .
- The Remuneration and Nominations committee determines the terms of service and remuneration of the Executive Directors and Corporate Officers and considers the appointments of Directors and Corporate Officers.
- The Corporate Social Responsibility Committee consists entirely of NEDs and provides a Board level forum for the regular review of external issues that have the potential for serious impact upon the Group's business and reputation.[96]

Lyttelton Port Company Limited

Annual Report and Corporate Governance Statement 2001

Risk Management Committee:

Reviews and considers issues relating to the protection of people and property in the achievements of the company's business goals and profitability. This includes considering the placement of an annual assurance programme and making appropriate recommendations to the Board. The Committee is also charged with checking that the Board and management are acting in compliance with all relevant environmental resource management legislation.[97]

National Archives of Australia

The audit committee is responsible for overseeing and reviewing arrangements for controls and operations generally, and for recommending and proposing action. To exercise this responsibility, the committee:

- reviews, critiques and reports on the Archives' internal and external audit plans, strategies reports and recommendations;
- reviews and evaluates the Archives' responses to audit reports;
- reviews and evaluates risk management strategies and fraud control plans;
- monitors legislative change, government policy, and other regulations in terms of their possible impact on the Archives;
- evaluates internal management and accounting controls;
- reviews accounting policies and disclosures in the annual financial statements; and
- reports on compliance breaches.

The Archives deal with manageable risk by adopting procedures as outlined in its Risk Management Plan, which incorporates the Disaster Preparedness Plans, Fraud Control Plan, Emergency Response Plan, and Business Recovery Plans. In 2001–02, the Archives is reviewing, coordinating and integrating the component plans. The Archives has transferred non-manageable risk to insurance providers Comcover and Comcare. Senior staff exercise risk management as appropriate.[98]

SEARS Canada Inc.

Corporate Governance

The board of directors is responsible to oversee the business and affairs of the Corporation and to act with a view to the best interests of the Corporation, providing guidance and direction

to the management of the Corporation in order to attain corporate objectives and maximise shareholder value.

The Board of Directors and the Audit and Corporate Governance, Compensation, and Nominating Committees of the Board are each responsible for certain corporate governance functions in accordance with their respective mandates. The Audit and Corporate Governance Committee is responsible for monitoring and guiding the corporate governance approach and practices of the Corporation.[99]

M. Matthey

Corporate Governance

There is a continuous process for identifying, evaluating and managing significant risks faced by the company which has been in place during the year under review and up to the date of approval of the annual report and accounts. The board regularly reviews this process.

The Group Control Manual, which is distributed to all group operations, clearly sets out the composition, responsibility and authority limits of the various board and executive committees and also specifies what may be decided without central approval. It is supplemented by other specialist policies and procedures manuals issued by the group, divisions and individual business units or departments. The high intrinsic value of many of the metals with which the group is associated necessitates stringent physical controls over precious metals held by the group.

The internal audit function is responsible for monitoring the group's systems of internal financial controls and the control of the integrity of the financial information reported to the board.[100]

BBC Worldwide

Annual Report and Accounts 2000

Corporate Governance

Risk Management – The board has responsibility for the identification and management of risks facing the business. Management updates their assessment of their exposure to risk, and the extent to which these risks are controlled, every four months. Management assessments are verified by visits from internal audit, which reports on this matter to the newly formed Corporate Risk Management Committee, which considers risk management across the BBC group as a whole.

Monitoring of controls – BBC Worldwide has a formally constituted Risk Management and Internal Control Committee (RMICC) comprising the Board of Directors with the Head of BBC Internal Audit (or Deputy) in attendance. This has responsibility for reviewing the effectiveness of BBC Worldwide's internal control environment and ensuring that existing controls and procedures are followed. It meets regularly to consider, inter alia, reports from internal and external audit. The BBC Internal Audit function undertakes regular testing of control systems under a plan agreed by the BBC's Audit Committee and the RMICC. The programme of testing, which is updated every four months, is based on assessment of key risks and issues. The results are reported to the RMICC.

External audit report – In addition to our audit of the financial statements, the directors have instructed us to review their Corporate Governance statement as if the group were required to comply with the Listing Rules of the Financial Services Authority in relation to these matters.

> We review whether the statement on page 25 reflects the group's compliance with the seven provisions of the Combined Code specified for audit review by those rules, and we report if it does not. We are not required to consider whether the Board's statements on internal controls cover all risks and controls, or to form an opinion on the effectiveness of the group's corporate governance procedures or its internal controls.[101]

Reuters

> Non-financial risks, including possible damage to Reuters' reputation as a leading news provider, or threats to the reliability of its computer systems, are examined by a Business Risks Steering Group which periodically reports to the board on the management of risks throughout the group. There is also a dedicated risk management function at Instinet. In 1997, Reuters established a compliance programme to consolidate and extend compliance activities . . . A Compliance Overview Group has been established, chaired by the Finance Director. Its members include the heads of the compliance group, business risks, the legal department and the internal audit department.[102]

The Reporting Reality

Published reports are only as good as the reliability of the information contained within them. Unfortunately, requiring companies to report on corporate governance compliance does not always mean the authoritative guidance has been adopted by the company. At times, a company will simply copy the standard wording used by those companies who are taking more of a lead in corporate governance reporting.

The Board and Directors

The board is responsible for reporting on their corporate governance arrangements. The IIA has provided a definition of the board:

> A board is an organization's governing body, such as a board of directors, supervisory board, head of an agency or legislative body, board of governors or trustees of a nonprofit organization, or any other designated body of the organization, including the audit committee to whom the chief audit executive may functionally report.

The UK's IoD has produced standards and guidelines for boards and directors and suggest that the boards should focus on four key areas:

1. establishing vision, mission and values;
2. setting strategy and structure;
3. delegating to management;
4. exercising accountability to shareholders and being responsible to relevant stakeholders.

The responsibilities of individual company directors have been documented by the IoD:

- determining the company's strategic objectives
- monitoring progress towards achieving the objectives and policies

- appointing senior management
- accounting for the company's activities to relevant parties eg shareholders

Statutory duties:

- a director must not put himself in a position where the interests of the company conflicts with his personal interest or his duty to a third party.
- a director must not make a personal profit out of his position as a director unless he/she is permitted to do so by the company.
- a director must act in what he/she considers is in the interests of the company as a whole, and not for any collateral purpose.

Directors are responsible for making sure the company fulfils its statutory duties (generally through the company secretary) . . . the main duty is the preparation of the accounts and report.

Directors are expected to display a certain amount of skill and exercise reasonable care in the performance of their work. In certain circumstances directors can be disqualified – eg wrongful trading (when insolvent) and fraudulent trading (defrauding the creditors).[103]

In the eyes of many officials charged with drafting corporate governance codes, the non-executive director (NED) represents the key to the future of corporate accountability. This all-seeing, all-knowing individual will examine the accounts, test the external auditor, watch over the board, align with the internal auditor, appraise the corporate strategy and ensure that enterprise-wide risk management is effectively imbedded within all parts of the organization. And at the same time be independent of the executive board members and protect the interests of all major stakeholders. No mean feat. The IoD have noted the contribution of NEDs:

There is no legal distinction between executive and non executive directors. Essentially the NED's role is to provide a creative contribution to the board by providing objective criticism . . . they bring to the board:

- independence
- impartiality
- wide experience
- special knowledge
- personal qualities

Responsibilities of NEDs:

- strategic direction – with a clearer and wider perspective
- monitoring performance of executive management
- communication – using outside contacts and opinions
- audit – it is the duty of the whole board to ensure that the company accounts properly to its shareholders by presenting a true and fair reflection of its actions and financial performance and that the necessary internal control systems are put in place and monitored regularly and rigorously
- remuneration of executive directors
- appointing directors

The demands of the NED role call for courage, integrity, common sense, good judgement, tenacity and to communicate with clarity, objectivity and brevity . . . business acumen . . . numeracy and the ability to gain an adequate understanding of the company's finance . . .

The contribution of NEDs can help to raise the level of discussion and improve the quality of decision-making on the board, thus increasing the chances of the company acting in the best interests of its long term security and prosperity.[104]

Meanwhile, the NEDs are seen by many as important components of corporate governance by institutional investors as they strive to ensure that their investments are being handled properly:

> Non-executive directors should not just be talking to the board directors. They should be spending part of their time visiting plants, talking to people at all levels and building up a picture of how the company is running[105]

The Chartered Institute of Management Accountants (CIMA) have prepared a paper that supports the use of NEDs and suggest that:

> Unlike a business 'mentor', a NED has a legally constituted position and vote on the board. The NED is therefore in a position to challenge the actions of the board should there be disagreement over the direction it wishes to take . . . The key to any successful appointment is for the board to be clear about what qualities they are looking for in a potential applicant. Many attributes may be desired – integrity, diplomacy, tact, experience of business, good judgement and financial and commercial acumen.[106]

This new thinking should be set against the history of NEDs where one illuminating description of the changing role of the NED appears in the following extract from the ACCA's *Accounting and Business Journal*:

> There was a time when a NED was seen as something you gave an old friend at Christmas. Anyone with a half decent career in the City behind them could virtually guarantee a comfortable semi-retirement with a handful of NED positions . . . the average NED of a FTSE 100 company receives around £35,000 for a few days a year work. But the difference today is that NEDs really do earn their money . . . they are expected to be truly independent and to act as an unofficial watchdog for investors and shareholders. Strictly speaking, NEDs have exactly the same legal responsibilities as company directors which are briefly:
>
> - A fiduciary duty to act honestly and in good faith.
> - A duty to exercise due skill and care.
> - Statutory duties, including preparation of accounts, a duty to employees and duties in relation to auditors.
>
> NEDS are not required to give continuous attention to company affairs. They are required to familiarise themselves with the company's affairs and should attend board meetings whenever they are reasonably able to do so.[107]

Things do not always go smoothly even where the NEDs have been able to acquire the demanding competencies required to discharge their role and responsibilities. Moreover, many NEDs sit on several company boards (and audit committees) and therefore may not have much time and energy to dedicate to each directorship. Andrew Chambers has noted the potential for conflict between executive and non-executive directors (NEDs):

> A running source of tension on the board may be the dividing line between executive and non-executive responsibilities. The finance director may feel that the chair of the audit committee, and the audit committee itself, is trespassing into his or her area of executive responsibility. Examples of this might be the general reporting by internal audit to the audit committee, the approval of an internal audit needs assessment by the audit committee, the commissioning of a special assignment to be conducted directly for the audit committee – and so on.[108]

The now infamous remarks from an outgoing president of the IoD reveal the real difficulties inherent in fulfilling the very demanding role and heightened expectations of non-executives:

> Lord Young, outgoing president of the IoD has called for NEDs to be abolished . . . The idea has come about that in some manner non-executives can second guess the executives, of course they can't. If management is not forthcoming, they can never even know, until it is far too late . . . Senior IoD officials have since clearly sought to distance themselves from his conclusions.[109]

Most corporate governance codes call for independent directors to take a lead on sensitive matters such as remuneration and accountability. But this is dependent on these directors being seen as really independent of the company. Many people feel that NEDs should have a stake in the company to motivate them to improve corporate performance, although whether this should include share options is open to debate:

> Should non-execs be rewarded with share options in the company? . . . Covering 68% of FTSE 100 companies, it (a survey) found that none offered share options to non-executives. In contrast, 69% of comparable US companies did so . . . Non-executive directors of the Houston energy trader (Enron) were rewarded with stock options. So they had an incentive to sanction related party transactions whereby losses were whisked from the accounts into special purpose entities. Back in the UK, non-executive failures had more to do with poor acquisitions, as at Marconi, than over-aggressive accounting . . . but I like one chairman's quote. 'Non-executive directors are not God's gift, they're not the answer to everything.' He declared. 'They are a device to provide part of the answer to some of the questions.' Quite so.[110]

The limitation of NEDs is generally accepted as part of the reality of business life. One question that springs to mind is 'When is an NED not an NED?' When they are not independent. This simple equation can at times be difficult to handle as the following extract illustrates:

> Shareholders were telling Stelios Haji-Ioannou last week that he had to leave the board of easy-Jet because he held too many shares to be an independent director. This week they were jumping up and down at the annual general meeting of insurance giant CGNU to protest against the board's decision to change the group's name to Aviva. This is not the way shareholders are expected to behave in this country. Stelios and Aviva may be legitimate issues in their different ways, but it is hard to see in either sufficient reason for the shareholders to take to the street. The fact that they are so agitated therefore suggests a deeper malaise. Shareholders are upset and want something. The question is what.[111]

Meanwhile back in 2002, the DTI review recognizes the importance of NEDs and states that:

> NEDs play a central role in the corporate governance of UK companies. From the point of view of UK productivity and competitiveness, the progressive strengthening of the role of NEDs is strongly desirable. The Combined Code already makes clear the principle that Boards include a balance of executive directors and NEDs (including independent NEDs) such that no individual or small group of individuals can dominate the Board's decision taking. (para. 4.15)

There are ongoing reviews of the role and responsibilities including a review by Derek Higgs reported in January 2003 (to the Chancellor of the Exchequer and the Secretary of State for

Trade and Industry), considering how to make best use of this scarce resource. Extracts from the draft follow:

The board

- The board is collectively responsible for promoting the success of the company by leading and directing the company's affairs. A description of the role of the board is proposed for incorporation into the Combined Code (the Code).
- The number of meetings of the board and of its main committees should be stated in the annual report, together with the attendance of individual directors. A description should be included in the annual report of how the board operates.
- The board should be of an appropriate size. At least half the members of the board, excluding the chairman, should be independent non-executive directors. There should also be a strong executive representation on the board.

The chairman

- The chairman has a pivotal role in creating the conditions for individual director and board effectiveness. The Review describes the role of the chairman and some of the attributes and behaviours of an effective chairman.
- The roles of chairman and chief executive should be separated and the division of responsibilities between the chairman and chief executive set out in writing and agreed by the board.
- A chief executive should not become chairman of the same company. At the time of appointment the chairman should meet the test of independence set out in the Review.

Role of the non-executive director

- A description of the role of the non-executive director is proposed for incorporation into the Code. Guidance is offered for non-executive directors on how to maximise their effectiveness.
- The non-executive directors should meet as a group at least once a year without the chairman or executive directors present and the annual report should include a statement on whether such meetings have occurred.
- Prior to appointment, potential new non-executive directors should carry out due diligence on the board and on the company to satisfy themselves that they have the knowledge, skills, experience and time to make a positive contribution to the board. Guidance on pre-appointment due diligence is offered.

The senior independent director

- A senior independent director should be identified who meets the test of independence set out in the Review. The senior independent director should be available to shareholders, if they have concerns that have not been resolved through the normal channels of contact with the chairman or chief executive.

Independence

- All directors should take decisions objectively in the interests of the company.
- A definition of independence is proposed for incorporation into the Code.

Recruitment and appointment

- There should be a nomination committee of the board to conduct the process for board appointments and make recommendations to the board.
- The nomination committee should consist of a majority of independent non-executive directors. It may include the chairman of the board, but should be chaired by an independent

non-executive director. A statement should be made in the annual report setting out the composition, terms of reference, and activities of the nomination committee and the process used for appointments.

- The nomination committee should evaluate the balance of skills, knowledge and experience on the board and prepare a description of the role and capabilities required for a particular appointment.
- On appointment, non-executive directors should receive a letter setting out what is expected of them.
- The nomination committee should provide support to the board on succession planning.
- Chairmen and chief executives should consider implementing executive development programmes to train and develop suitable individuals in their companies for future director roles.
- The board should set out to shareholders why they believe an individual should be appointed to a non-executive director role and how they meet the requirements of the role.
- Proposals are made to broaden the pool of candidates for non-executive director appointments, including more executive directors and senior executives from other companies and directors of private companies, as well as advisors and those from other backgrounds.
- A small group of business leaders and others will be set up to identify how to bring to greater prominence candidates for non-executive director appointment from the non-commercial sector.
- The Review offers guidance on the process for the appointment of a new chairman.

Induction and professional development

- A comprehensive induction programme should be provided to new non-executive directors and is the responsibility of the chairman, supported by the company secretary.
- The chairman should address the developmental needs of the board as a whole with a view to enhancing its effectiveness. Resources should be provided for developing and refreshing the knowledge and skills of directors.
- The performance of the board, its committees and its individual members, should be evaluated at least once a year. The annual report should state whether such performance reviews are taking place and how they are conducted.
- Supported by the company secretary, the chairman should assess what information is required by the board. Non-executive directors should satisfy themselves that they have appropriate information of sufficient quality to make sound judgements.
- The company secretary should be accountable to the board as a whole, through the chairman, on all governance matters.

Tenure and time commitment

- A non-executive director should normally be expected to serve two three-year terms, although a longer term will exceptionally be appropriate.
- On appointment, non-executive directors should undertake that they will have sufficient time to meet what is expected of them, taking into account their other commitments. If a non-executive director is offered appointments elsewhere, the chairman should be informed before any new appointment is accepted.
- The nomination committee should annually review the time required of non-executive directors. The performance evaluation should assess whether non-executive directors are devoting enough time to fulfil their duties.
- A full time executive director should not take on more than one non-executive directorship, nor become chairman, of a major company. No individual should chair the board of more than one major company.

Remuneration

- The remuneration of a non-executive director should be sufficient to attract and fairly compensate high quality individuals. It may comprise an annual fee, a meeting attendance fee, and an additional fee for the chairmanship of committees. Non-executive directors should have the opportunity to take part of their remuneration in the form of shares.
- Non-executive directors should not hold options over shares in their company. If, exceptionally, some payment is made by means of options, shareholder approval should be sought in advance and any shares acquired by exercise of the options should be held until one year after the non-executive director leaves the board.
- Where a company releases an executive director to serve as a non-executive director elsewhere, it should include in its remuneration policy report whether or not the director will retain the related remuneration and, if so, its amount.

Resignation

- Where a non-executive director has concerns about the way in which a company is being run or about a course of action proposed by the board, these should be raised with the chairman and their fellow directors. Non-executive directors should ensure their concerns are recorded in the minutes of the board meetings if they cannot be resolved.
- On resignation, a non-executive director should inform the chairman in writing, for circulation to the board, of the reasons for resignation.

Audit and remuneration committees

Sir Robert Smith's recommendations on audit committees are endorsed.

- The remuneration committee should comprise at least three members, all of whom should be independent non-executive directors. It should have published terms of reference. The Review offers a summary of the principal duties of the remuneration committee.
- The remuneration committee should have delegated responsibility for setting remuneration for all executive directors and the chairman. The committee should also set the level and structure of compensation for senior executives. The committee should be responsible for appointing remuneration consultants.
- No one non-executive director should sit on all three principal board committees (audit, nomination and remuneration) simultaneously.

Relationships with shareholders

- All non-executive directors, and in particular chairmen of the principal board committees, should attend the Annual General Meeting (AGM) to discuss issues that are raised in relation to their role.
- The senior independent director should attend sufficient of the regular meetings of management with a range of major shareholders to develop a balanced understanding of the themes, issues and concerns of shareholders. The senior independent director should communicate these views to the non-executive directors and, as appropriate, to the board as a whole.
- Boards should recognise that non-executive directors may find it instructive to attend meetings with major investors from time to time and should be able to do so if they choose. Moreover, non-executive directors should expect to attend such meetings if requested by major investors in the company.
- On appointment, meetings should be arranged for non-executive directors with major investors, as part of the induction process.
- A company should state what steps it has taken to ensure that the members of the board, and in particular the non-executive directors, develop a balanced understanding of the views of major investors.

- The Review endorses the Government's approach to more active engagement by institutional shareholders with the companies in which they invest, and the Institutional Shareholder Committee's (ISC) code of activism. Institutional investors should attend AGMs where practicable.

Smaller listed companies: The recommendation that no one individual should sit on all three principal board committees at the same time should not apply to smaller listed companies. With this exception, there should be no differentiation in the Code's provisions for larger and smaller companies. It may take more time for smaller listed companies to comply fully with the Code and it is recognised that some of its provisions may be less relevant or manageable for smaller companies.

NEDs require a knowledge of the business, a knowledge of corporate governance (and corporate strategy and performance management) and an understanding of the role of the NED and contributions that can be made; and more than anything, the ability to remain objective in both helping install corporate governance and challenging the decisions made by the board on related matters – which frowns on cross-directorships where companies have directors who sit as NEDs on other companies' boards who repay the favour in return. In addition, they should have had no recent association with the companies' advisors and executives. There is also a need to ensure NEDs have sufficient time to address company business and that the number of directorships they hold is restricted to a manageable number. Stronger corporate governance codes promote a balanced board where a chair ensures that the board performs properly while the CEO ensures that the company performs likewise. In other words, the role of chair and CEO are split so that the CEO does not have unfettered power over the boardroom. The Cadbury Report acknowledges the importance of the board chairman:

> The chairman's role in securing good corporate governance is crucial. Chairmen are primarily responsible for the working of the board, for its balance of membership subject to board and shareholders' approval, for ensuring that all relevant issues are on the agenda, and for ensuring that all directors, executive and non-executives alike, are enabled and encouraged to play their full part in its activities. Chairmen should be able to stand sufficiently back from the day-to-day running of the business to ensure that their boards are in full control of the company's affairs and alert to their obligations to their shareholders. (para. 4.7)

The IoD have, in the past, prepared standards for the role of chair:

- act as the company's leading representative
- to take the chair and general and board meetings
- to take a leading role in determining the composition and structure of the board.[112]

Audit committees are important in corporate governance but they are only committees of the main board, and are dealt with in a separate section of this chapter. Some writers argue that there should be a further layer in a company to monitor the board:

> After the Enron and Worldcom scandals, there is now a familiar call to tweak accounting/ auditing standards and strengthen the role of the non-executive directors. We have heard all this before. After BCCI, Maxwell, Polly Peck, Transtec and other scandals, Cadbury, Hampel and other reviews were wheeled out, with predictable results. Instead of democratising corporations and making them accountable to ordinary people, they further concentrated economic, social and

> political power in relatively few hands . . . In the post-Enron world, attention should be focused on bringing corporate power under democratic control. Replacing the unitary board of major companies with a two-tier board of directors could make a modest start. The second tier should consist entirely of full-time non-execs that are directly elected by stakeholders (employees, bank depositors, and investors). Its task should be to formulate strategy, standards of ethical conduct, wealth distribution, accountability and probity.[113]

This arrangement would be similar to the two-tier boards in some European countries such as Germany where the executive board runs the company while the supervisory board, half of whose members are employees, supervises and advises the executive board and is responsible for sensitive areas such as executive board members' performance-based remuneration. Whatever the adopted format, the board need to appreciate their responsibilities to balance performance with propriety and be committed to a good dialogue with shareholders and stakeholders generally. This requires, more than anything else, new attitudes and not just rules regarding formal reporting requirements. Increasingly, the upwards responsibility to stakeholders is matched by a downwards responsibility for ensuring risks to the business are properly understood and managed throughout the organization. The accountability message is being driven home and the National Association of Corporate Directors has noted that: 'An increasing number of corporate directors of US public companies are becoming advocates for greater board accountability and independence, favouring such actions as board and director evaluations, executive sessions and the establishment of independent compensation committees.'[114] Coming off the scandals of 2002, by November 2002 the US governance rules were revamped to tighten up on accounting and accountability through the Sarbanes-Oxley Act 2002 which included the following extracted points:

1. Management must publicly state its responsibility for internal control and provide an assessment of the effectiveness of the internal control structure.
2. The principal executive officer/s and the principal finance officer/s will be required to certify in each annual or quarterly report that the signing officers of the report: are responsible for establishing and maintaining internal controls; have designed such internal controls to ensure that material information relating to the organisation is made known to them; have evaluated the effectiveness of the organisation's internal controls within 90 days prior to the report; and have presented in the report their conclusions about the effectiveness of their internal controls based on their evaluation as of that date.
3. These officers also have to disclose to the auditors and the audit committee: all significant deficiencies in the design or operation of internal controls which could adversely affect the organisation's ability to record, process, summarise, and report financial data and have identified for the auditors any material weaknesses in internal controls; and any fraud, whether or not material, that involves management or other employees who have significant role in the organisation's internal controls.
4. They also have to indicate whether or not there were significant changes in internal controls or in other factors that could significantly affect internal controls subsequent to the date of their evaluation, including any corrective actions with regard to significant deficiencies and material weaknesses.
5. The company's external auditors have to attest to and report on management's assertions about internal control and the organisation's Chief Audit Executive (the US equivalent of head of internal audit) will be called upon to assure management that systems and processes are operating as planned.
6. The external auditor also has to describe in each audit report the scope of its testing of the internal control structure and procedures and give a description, at a minimum, of material

weaknesses in such internal controls, and of any material non-compliance found on the basis of such testing.[115]

Meanwhile the rules for companies listed on the New York Stock Exchange (NYSE) were required to line up with a likewise tighter set of provisions:

1. Listed companies must have a majority of independent directors.
2. In order to tighten the definition of 'independent director' for purposes of these standards . . .
3. To empower non-management directors to serve as a more effective check on management, the non-management directors of each company must meet at regularly scheduled executive sessions without management.
4. (a) Listed companies must have a nominating/corporate governance committee composed entirely of independent directors. (b) The nominating/corporate governance committee must have a written charter . . .
5. (a) Listed companies must have a compensation committee composed entirely of independent directors. (b) The compensation committee must have a written charter . . .
6. Add to the 'independence' requirement for audit committee membership the requirement that directors' fees are the only compensation audit committee members may receive from the company.
7. (a) Increase the authority and responsibilities of the audit committee, including granting it the sole authority to hire and fire independent auditors, and to approve any significant non-audit relationship with the independent auditors. (b) The audit committee must have a written charter . . . (c) Each listed company must have an internal audit function.
8. To increase shareholding control over equity-compensation plans, shareholders must be given the opportunity to vote on all equity-compensation plans, except inducement options, plans relating to mergers or acquisitions, and tax qualified and excess benefit plans.
9. Listed companies must adopt and disclose corporate governance guidelines.
10. Listed companies must adopt and disclose a code of business conduct and ethics for directors, officers and employees, and promptly disclose any waivers of the code for directors or executive officers.
11. Listed foreign private issuers must disclose any significant ways in which their corporate governance practices differ from those followed by domestic companies under NYSE listing standards.
12. Each listed company CEO must certify to the NYSE each year that he or she is not aware of any violation by the company of NYSE corporate governance listing standards.
13. The NYSE may issue a public reprimand letter to any listed company that violates an NYSE listing standard.[116]

Unfortunately, the focus was on control over financial reporting.

2.6 The External Audit

External audit fits into the corporate governance jigsaw by providing a report on the final accounts prepared by the board. They check that these accounts show a fair view of the financial

performance of the company and its assets and liabilities at the end of the accounting year. The corporate governance model can be further developed to include an additional layer of accountability through the external audit process as in Figure 2.4.

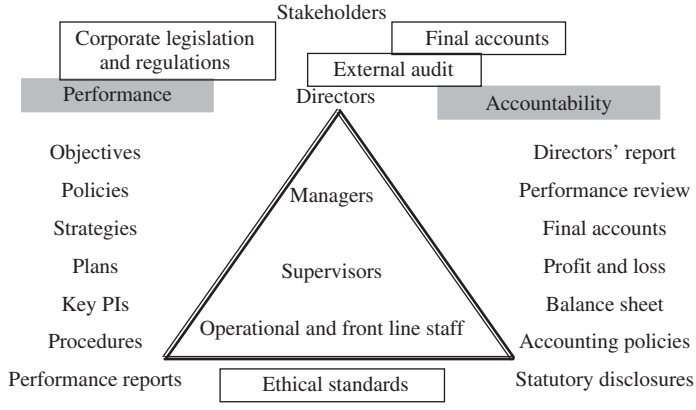


FIGURE 2.4 Corporate governance (4).

The Different Objectives

The starting place is to clearly set out the different objectives of internal and external audit:

The external auditor The external auditor seeks to test the underlying transactions that form the basis of the financial statements. In this way, they may form an opinion on whether or not these statements show a true and fair view. Reliance may be placed on those systems that produce the accounts so that less testing will be necessary where the system is found to be sound. The systems are, however, perceived as a short-cut to examining all the financial transactions for the period in question. The price of missing important items in the accounts can be high as one news article demonstrates:

> PW is to take over from the existing firm as auditor of the beleaguered DIY retailer Wickes . . . whose profits had been overstated by over $50 m in recent years. Wickes did not intend to take action against its auditors over its failure to spot the deception which took place in Wickes buying department, with the collusion of selling departments in supplier companies which provided false documentation.[117]

The internal auditor The internal auditor, on the other hand, seeks to advise management on whether its major operations have sound systems of risk management and internal controls. To this end, the auditor will test the resultant transactions to confirm the evaluation and determine the implications of any systems' weaknesses. These systems are primarily designed to ensure the future welfare of the organization rather than accounting for its activities. It should be clear from the above that the external auditor uses systems as a short-cut to verifying the figures in the accounts. In contrast, the internal auditor is primarily concerned with all systems of control that enable organizational objectives to be met. Note that in the public sector, the National Audit Office and the Audit Commission, as well as their role in final accounts, also examine operational matters and value-for-money issues. In addition, firms of auditors may be asked to undertake various consultancy projects in addition to their external audit role.

Background to External Audit

There are features of the private sector external auditor's role that may be noted to help understand the relationship between internal and external audit:

- External auditors are generally members of CCAB professional accountancy bodies and are employed under the companies apostrophe legislation to audit the accounts of registered companies.
- They are appointed annually at the annual general meeting by their clients, the shareholders.
- Their remuneration is fixed at the general meeting.
- They have a right to attend general meetings to discuss any audit-related matters.
- They have a right of access to all books, information and explanations pertaining to the financial statements.
- In a limited company they can be removed by ordinary resolution with special notice.
- They cannot be officers, corporations or partners or employees of officers.
- In the event of their resignation they have to provide a statement of circumstances to the new incoming auditor that will document any specific problems with the audit cover.
- Where there is a problem with the accounts the auditor will fashion a suitable report to reflect the nature of the problem.

External audit will arrive at an opinion using the criteria in Figure 2.5.

	Effect on the accounts	
Auditor's view	Material	Fundamental
Uncertainty	Subject to	Disclaimer
Disagreement	Except for	Adverse

FIGURE 2.5 External audit report format.

In this way the external auditor will form an opinion on the accounts based on the adopted position. Note that the public sector and not-for-profit organizations will also be subject to external audits.

The Main Similarities

The main similarities between internal and external audit are as follows:

- Both the external and internal auditor carry out testing routines and this may involve examining and analysing many transactions. Where these revolve around financial systems they may appear to be very similar, particularly for the operational staff who have to supply the required information to assist the audit in hand. There are many auditors who have tried to explain the different roles of the two functions to a confused manager who has seen both teams perform what appears to be exactly the same work. As testament to this, one will recall the many times where a client has handed a document to the internal auditor, who after much confusion is able to work out that the document actually belongs to the external audit team. This confusion is enhanced where the size of the audit means that the external audit team is located within

the organization. Having said this, there are many ways that audit testing programmes applied to financial systems appear to be very similar and this does bring the two audit functions closer together in terms of working methodologies.

- Both the internal auditor and the external auditor will be worried if procedures were very poor and/or there was a basic ignorance of the importance of adhering to them. Obviously the external auditor will be involved in matters that impinge on the financial statements, although they may comment on the overall arrangements for setting standards and direction. Internal audit will tend to take this concept further in an attempt to promote suitable controls. The auditor's work is dependent on people doing things in the way that is laid down by the organization and they will not take this factor for granted without applying appropriate compliance tests.
- Both tend to be deeply involved in information systems (IS) since this is a major element of managerial control as well as being fundamental to the financial reporting process. New computerized developments that impact on the figures presented in the final accounts must incorporate basic controls to ensure the integrity of the database and ensuing reports. IS audit is a term applied to both external and internal audit as a follow-up to this principle. A good IS auditor may work in both types of audit roles throughout his/her career, as the skills applied to this type of work are wholly transferable. Take as an example computer interrogation routines that seek to identify correct functionality or say duplicate accounts; these may be applied to financial information systems by both external and internal audit although from different perspectives. The external auditor will seek to assess whether the information supplied by the computer that forms the basis of figures for the accounts is correct. The internal auditor will be concerned that the computer generates correct reports that enable management to achieve their objectives efficiently. Obviously the internal auditor will consider all major systems that impact on organizational objectives as opposed to just the accounting-based ones. This makes for a concentration of resources on corporate managerial controls such as the systems development life cycle applied to new and developing computerized systems.
- Both are based in a professional discipline and operate to professional standards. The external auditor's work is in the main covered by the Auditing Practices Board (APB) auditing standards, which cater for matters such as starting an engagement, planning work and carrying out the required tasks. In the UK, the internal auditor makes reference to either the IIA standards or equivalent internal auditing standards. There is one key difference in the form of an added impetus to subscribe properly to auditing standards that applies to the external auditor. This is the ever-present threat of legal action that may be taken by a client or a third party who has relied on the financial statements and suffered a loss as a result. The ability to prove that one has operated to professional standards is almost a prerequisite to a successful defence against any claims of professional negligence. The internal auditor has two main forces that encourage compliance with professional standards. These appear in the form of the CAE's stance on this issue and the quality assurance procedures that should call for a review of compliance done either in-house or through external resources. The key point, however, is the view that both internal and external audit should seek to adhere to formal auditing standards that should form the foundation of their work. This would be translated perhaps as an in-house audit manual supported by suitable training and development programmes.
- Both seek active cooperation between the two functions. IIA standards cover this point while the external auditor has a remit, through APB guidelines, to place some reliance on the internal auditor's work wherever possible. This cooperation should operate on an equal footing and is partly designed to avoid embarrassing situations where both teams turn up at the same location at the same time.

- Both are intimately tied up with the organization's systems of internal control. Controls and the way they are interfaced with the organization's operational arrangements should be seen as an important concern, which is fundamental to the audit role. Considerations relating to authorization, segregation of duties, good documentation, audit trails, sound information systems, and supervision all fall under the remit of control systems that are key to the success of the business in hand. There is one external audit view that proposes the use of extended interrogation software to perform 100% testing of financial systems and so moves away from the need to place any great reliance on controls. This, however, is based on the narrow definition of controls used by external audit based on the output from accounting systems being more or less correct. We can contrast this with the wider internal audit view on controls that considers them to be mechanisms that promote the achievement of organizational objectives. The importance of sound controls has been given greater recognition recently by the external audit world with the general acceptance of this issue as part of the annual report issued by the directors. To this end we would expect the internal and external auditor to move closer together in relation to controls over financial systems. In practice we may speculate whether internal audit should have a key role in control evaluation by supporting relevant statements that appear in the annual report and accounts. The APB guidelines on placing reliance on internal audit may need to be reviewed to reflect this concept.
- Both are concerned with the occurrence and effect of errors and misstatement that affect the final accounts. This is a key concern of the external auditor where it has an impact on the audit report that is issued after reviewing the items set out in the final accounts. In this situation, the internal auditors would be interested in the system's weaknesses that have led to the resultant errors in contrast to the external auditor's interest in the effect of incorrectly stated figures. Where there is good cooperation between the two functions, we may expect a great deal of close working to identify and resolve such problems.
- Both produce formal audit reports on their activities. The external auditor has tended to report on an exception basis where comments relate specifically to the type of audit opinion that is provided. More recently audit standards require more information in audit reports that provide a more rounded view of work done and responsibilities. The problem for the external auditor is that the more that is said in a report the more the writer can be held to account. The internal audit report can be differentiated by its resemblance to the more conventional type of report with a formal structure, i.e. a beginning, middle and end. This can become a detailed document for larger audits although one would expect an executive summary to provide a brief statement of opinion, making it closer to the model used by the external auditor. Notwithstanding the differences in the report formats, we can conclude that both sets of auditors have to assume the discipline of formally reporting their findings and carrying out their work with this obligation in mind.

The Main Differences

There are, however, many key differences between internal and external audit and these are matters of basic principle that should be fully recognized:

- The external auditor is an external contractor and not an employee of the organization as is the internal auditor. Note, however, that there is an increasing number of contracted-out internal audit functions where the internal audit service is provided by an external body. In fact this external body is likely to be the same type of organization (e.g. firm of accountants)

as those that supply the external audit services. Having said this there is a third model that is being increasingly applied that involves a small in-house internal audit team supplemented by an outsourced contract that covers more routine audits. As such we are still dealing with internal auditors who are normally employees of the company. There is one further qualification to this where audit consortia are involved, as is popular in the UK's NHS; this is akin to an externally provided internal audit service.

- The external auditor seeks to provide an opinion on whether the accounts show a true and fair view. Whereas internal audit forms an opinion on the adequacy and effectiveness of systems of risk management and internal control, many of which fall outside the main accounting systems, it is important to get this concept clearly in mind and an illustration in Figure 2.6 may assist.

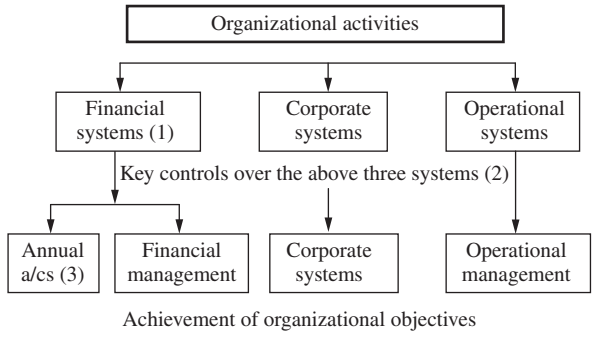


FIGURE 2.6 Auditing controls versus accounts.

The three key elements of this model are:

1. Financial systems may be considered by the external auditor as a short-cut to verifying all the figures in the accounts to complete the audit process. The internal auditor will also cover these systems as part of the audit plan.
2. Overall risk management arrangements are the main preoccupation of the internal auditor who is concerned with all those controls fundamental to the achievement of organizational objectives.
3. The final accounts are the main preoccupation of the external auditor who is concerned that the data presented in the accounts present a true and fair view of the financial affairs of the organization.

- It should be clear that the external audit role is really much removed from the considerations of the internal auditor both in terms of objectives and scope of work. The fact that there is some overlap in respect of controls over the accounting arrangements must be set within the context of these major differences.
- External audit is a legal requirement for limited companies and most public bodies, while internal audit is not essential for private companies and is only legally required in parts of the public sector. Much of the external auditor's work is prescribed in outline by law. To an extent even working practices are affected by case law dealing with claims of professional negligence against the auditor. Rights, responsibilities and the role of external audit are found in legislation that contains clear definitions that are well understood by the business community. The world of the internal auditor, on the other hand, was shrouded in mystery and may not be fully appreciated by management. The different methodologies applied by various internal audit functions and the fact that they need not necessarily be aligned to a professional body also make it hard to develop one universal model of internal auditing that can be held up as

an agreed standard. We may go on to suggest that the external auditor is more accepted by society than the internal audit counterpart as a result of the position we have just described. Unfortunately, there are many internal auditors who can only get the attention of the business community by making a mention of the importance of fraud investigations as a way of defining their role in society so as to avoid complicated discussions on other more significant aspects of their work. External auditors, on the other hand, have no need to enter the realms of conceptualization to explain their main role in society.

- IA may be charged with investigating frauds, and although the external auditors will want to see them resolved, they are mainly concerned with those that materially affect the final accounts. While there is a growing recognition of the external audit role in fraud investigations, the truth is that tackling fraud is not only hard work but also very resource intensive. Referring matters to internal audit is one good way of managing this issue if it comes about. Accordingly, some internal auditors tend to claim this area as its own. In the public sector where probity is seen as a key issue, there is generally a need to investigate all occurrences and/or allegations of fraud even where they go back some time. In the private sector this type of work will tend to be at the behest of the board of directors. In some cases the fraud aspects of organizational affairs will fall under specially designated security officers.
- Internal auditors cover all the organization's operations whereas external auditors work primarily with those financial systems that have a bearing on the final accounts. This point should not be underestimated since if external audit spends a great deal of time on financial systems it may result in the IA function dealing primarily with managerial/operational areas. If this is the case, the internal auditor may well commit only a small level of resources to the financial arena. Although this type of arrangement does depend on a close cooperation of the two audit functions, it also creates a clear differentiation in the two work areas that will tend to move them further apart in the long term. It also moves away from the alternative model where internal audit work is used primarily to allow a reduction in the level of external audit cover in designated areas. Reverting to the previous example, an exaggeration of the separation of systems into financial and others, in line with the different roles of external and internal audit, may allow the latter function to assume a fuller identity in its own right.
- IA may be charged with developing VFM initiatives that provide savings and/or increased efficiencies within the organization. Interestingly, this may also apply to the external auditor under the consultancy head (although the level of consultancy provided by the external auditor is restricted so as not to provide a conflict of interests). It also applies to some external auditors in the public sector (e.g. Audit Commission and National Audit Office). Generally speaking though, internal audit will be concerned with operational efficiency while the external audit function has no remit to delve into these areas of organizational activities.
- The internal auditor reviews systems of internal control in contrast to the external auditor who considers whether the state of controls will allow a reduced amount of testing. As such, external audit work is directed at the transactions that occurred within a past period in contrast to the future impact of good systems. As an example, the internal auditor may be concerned with the efficiency and effectiveness of the organization's marketing systems whereas there is no clear role for external audit in this area.
- Internal audit works for and on behalf of the organization whereas the external auditor is technically employed by and works for a third party, the shareholders. This is an important difference in that the client base has a great deal of influence on the audit role and reporting arrangements. The external auditor is clearly reporting on the organization's management as a fundamental part of their role. It is the board who approve the accounts, and society views the external audit function as a direct check over the figures on the basis that it is not ideal to rely on the unchecked accounts as they stand. The internal auditor does not have this

distinct philosophy for protection as it is the management who decides to employ an internal auditor, not to check on them, but to seek improvements to risk management systems. The point though is, having identified weaknesses, the internal auditor has no third party to go to if there is a lack of effective action to remedy these weaknesses. The internal auditor reports to the people in front of him/her, not some unseen force that periodically convenes as a group of shareholders watching over the organization with interest and ultimate authority. The theory is that an audit committee of NEDs fulfils this role, although the executive directors and chief executive do tend to have a great influence on this forum and so diminish its capacity as an ultimate control over the organization. This difference in reporting lines in turn creates a contrasting type of independence in that the external auditor is independent from the organization while internal audit is independent from the operations being reviewed. There are pressures on the external auditor particularly for owner-run registered companies that can impair the level of audit independence. There are also time pressures that can lead to junior staff doing limited work in poorly managed firms of auditors although the drive for quality assurance procedures does diminish the frequency of this type of scenario.

- The internal audit cover is continuous throughout the year but the external audit tends to be a year-end process even though some testing may be carried out during the year. Having said this, some larger organizations have a permanent external audit presence who provide year-round coverage of account verification and substantiation. For smaller companies one might imagine the external auditor arriving at the finance department after the accounts have been closed and producing a suitable report after the requisite period of audit work. This is very different from the full-time internal auditor who is consumed by the organizational culture as the years pass by, and colleagues across all departments become personal friends. We may be tempted to argue that the internal auditor is as such 'playing at auditing' as the years grow closer to retirement, if this did not expose a complete misunderstanding of the internal audit role.

It is possible to outline the key differences in Table 2.1.

TABLE 2.1 Internal versus external audit.

Factor	*Internal audit*	*External audit*
Objectives	Sound risk management and controls	Accounts = true and fair view
Scope of work	Overall systems: VFM, fraud, MIS and compliance	Accounts, profit and loss a/c, balance sheet, annual report and financial systems
Independence	From operations by professionalism and status	From company via statutory rights and APB codes
Structure	Varies: CAE, managers, seniors and assistants	Partners, managers, seniors and trainees
Staff	Competent persons trained in internal auditing	Qualified and part qualified accountants
Methodology	Risk-based systems-based audits, assurances and consulting work	Vouching and verification and some use of risk-based systems approach
Reports	Comprehensive structured reports to management and the audit committee and brief executive summaries	Brief standardized published reports to shareholders and users of accounts
Standards	IIA and/or other	Various APB requirements
Legislation	Generally not mandatory apart from parts of public sector, but encouraged in most sectors	Companies legislation and various public sector statutes
Size	Only larger organizations	All registered companies and public sector (small companies may have exemptions)

The Auditing Practices Board (APB) Statement

Because IA reviews systems and carries out testing routines it may produce much work that the external auditor might find useful. Reliance on internal audit's work reduces the external audit (EA) workload and may lead to lower fees. The APB has provided guidance on this matter that includes the following: external audit needs to assess the adequacy of IA before relying on its work and so reducing its own. Accordingly it will need to consider the following:

1. The IA work should be properly recorded.
2. The IA work should be properly controlled.
3. IA should be adequately independent.
4. The scope of the IA work should be sufficiently wide.
5. IA should have sufficient resources.
6. IA should be competent.
7. IA should carry out its work with due professional care.

Only where IA meets the above criteria may the external auditor restrict the amount of work based on the IA cover. In fact in a number of local authorities the district auditor (DA) has asked IA to undertake testing programmes of various central government claims before the DA signs the claim off. The budget for EA services is reduced accordingly. On the one hand, this shows a level of confidence in internal audit that should be taken as a compliment. The downside though is the creeping view that IA is there simply to back up the all-important external auditor. IIA standard 2050 covers coordination:

> The chief audit executive should share information and coordinate activities with other internal and external providers of assurance and consulting services to ensure proper coverage and minimize duplication of efforts.

Practice Advisory 2050-1 discusses the way the internal audit (IA) and external auditor's work can be coordinated:

> Oversight of the work of external auditors, including coordination with the internal audit activity, is the responsibility of the board. Coordination of internal and external audit work is the responsibility of the chief audit executive (CAE). The CAE obtains the support of the board to coordinate audit work effectively.
>
> Organizations may use the work of external auditors to provide assurance related to activities within the scope of internal auditing. In these cases, the CAE takes the steps necessary to understand the work performed by the external auditors, including:
>
> - The nature, extent, and timing of work planned by external auditors, to be satisfied that the external auditors' planned work, in conjunction with the internal auditors' planned work, satisfies the requirements of Standard 2100.
> - The external auditor's assessment of risk and materiality.
> - The external auditors' techniques, methods, and terminology to enable the CAE to (1) coordinate internal and external auditing work; (2) evaluate, for purposes of reliance, the external auditors' work; and (3) communicate effectively with external auditors.
> - Access to the external auditors' programs and working papers, to be satisfied that the external auditors' work can be relied upon for internal audit purposes. Internal auditors are responsible for respecting the confidentiality of those programs and working papers.

1. The external auditor may rely on the work of the internal audit activity in performing their work. In this case, the CAE needs to provide sufficient information to enable external auditors to understand the internal auditors' techniques, methods, and terminology to facilitate reliance by external auditors on work performed. Access to the internal auditors' programs and working papers is provided to external auditors in order for external auditors to be satisfied as to the acceptability for external audit purposes of relying on the internal auditors' work.

It may be efficient for internal and external auditors to use similar techniques, methods, and terminology to coordinate their work effectively and to rely on the work of one another. Planned audit activities of internal and external auditors need to be discussed to ensure that audit coverage is coordinated and duplicate efforts are minimized where possible. Sufficient meetings are to be scheduled during the audit process to ensure coordination of audit work and efficient and timely completion of audit activities, and to determine whether observations and recommendations from work performed to date require that the scope of planned work be adjusted.

1. The internal audit activity's final communications, management's responses to those communications, and subsequent follow-up reviews are to be made available to external auditors. These communications assist external auditors in determining and adjusting the scope and timing of their work. In addition, internal auditors need access to the external auditors' presentation materials and management letters. Matters discussed in presentation materials and included in management letters need to be understood by the CAE and used as input to internal auditors in planning the areas to emphasize in future internal audit work. After review of management letters and initiation of any needed corrective action by appropriate members of senior management and the board, the CAE ensures that appropriate follow-up and corrective actions have been taken. The CAE is responsible for regular evaluations of the coordination between internal and external auditors. Such evaluations may also include assessments of the overall efficiency and effectiveness of internal and external audit activities, including aggregate audit cost. The CAE communicates the results of these evaluations to senior management and the board, including relevant comments about the performance of external auditors.

This cooperation between IA and EA is important and better coordination can also be encouraged by considering the following techniques:

1. A common audit methodology A close cooperation can result from adopting a common approach to audit work. This may, for example, revolve around a systems-based approach where one would seek to ascertain, evaluate, test and then report the relevant findings. In practice the policy would work better if it were based around developing clear but different methodologies that are understood by both audit functions. This recognizes the differences in objectives, scope and approach to work that will attach to each type of audit, and deals with the difficulty in achieving a universal approach. So long as working methodologies are defined and publicized, then a basic appreciation should result which in turn would underpin any drive towards harmonization.

2. Joint training programmes Again fully integrated training programmes, as an ideal, are not possible due to the different nature of the two audit functions. A policy of joint training can nonetheless be applied so long as this is limited to general audit techniques. These include flowcharting, statistical sampling, database interrogation, transactions testing, interviewing skills, control evaluation and so on. Time and resource may be rationalized where this approach is adopted. The disadvantage is the many limitations that must be placed on this approach since many of the techniques dealt with would have to be discussed as conceptual matters, with no link into audit objectives (that do not really reconcile).

3. Joint planning of audit work This is the single most useful policy in terms of coordinating internal and external audit. Harmonization of the planning task is fundamental in this respect.

There are several levels to which audit planning may be interfaced as Figure 2.7 suggests.

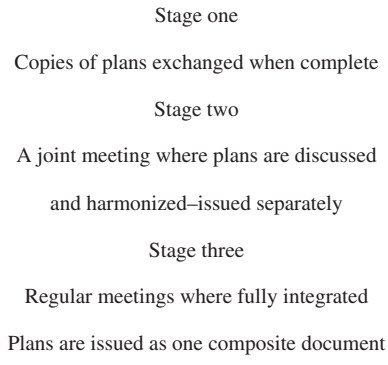


FIGURE 2.7 Interfaced audit planning.

The stages move from one through to three to reflect an increasingly greater degree of interface between internal and external audit. At the extreme it can result in one planning document being prepared for the organization. This is more relevant in the public sector where EA tends to assume a role in securing VFM. Stage one consists of a common courtesy where plans are exchanged, which in fact involves two sublevels where draft plans are given (which can as a result be altered). This is in contrast to the less integrated stance where only finalized plans are provided.

4. Direct assistance with each other's projects A swap of resources creates further cooperation as the available audit skills base is added to as and when required. This can allow, as an example, an external information systems auditor to run interrogation software to support the internal auditor's review of a large financial system. IA may in turn complete a suitable testing programme that enables external audit to substantially reduce work in the area in question. Note that some of these issues have been mentioned earlier.

5. Exchanging reports This is a simple method of keeping each side informed although it is more relevant within a public sector environment. Unfortunately what at first appears straightforward may involve an amount of political manoeuvring where each side applies special rules for confidential reports or reports that have not reached final report status. A more explicit statement of cooperation occurs where pre-report stage material, such as the agreed terms of reference for the ensuing audit, is also exchanged.

Another view of audit cooperation was published in *Internal Auditing* and suggests that there are several different models that can be applied:

1. **Coexistence** – pursue separate missions, risk analysis, audit plan execution are developed and performed independently as separate and distinct activities.
2. **Coordination** – independently develop but share information on risk analysis, some attempt to coordinate audit plans, if joint auditing is performed the EA typically tends to determine when and where such joint activities take place.

3. **Integration** – share risk models and audit plans, extensive joint planning.
4. **Partnering** – comprehensively define corporate audit needs and expectations and meet those requirements through a joint and integrated effort, shared mission encompassing financial, substantive, compliance and systems auditing.

> It is our hope that internal and external audit groups will continue working together to determine how to best increase the efficiency and effectiveness with which the internal and external auditors coordinate their efforts to complete the financial statement audit.[118]

In terms of public sector audit, Lord Sharman has suggested that:

> 'A close relationship between internal and external auditors helps strengthen the internal audit function by bolstering the latter's independence, and providing additional justification for management to take internal audit concerns seriously.' Sharman's report also says that the appointment of NEDs to sit on departmental boards is a welcome development.[119]

The External Audit Approach

An APB paper called 'The Audit Agenda' was prepared some time ago to strengthen the role of EA:

- It recognizes that the audit requirements of listed and owner-managed companies are different.
- It advocates that an extended audit should apply to listed companies and major public companies. Here compliance with the Cadbury code of corporate governance becomes a major concern.
- It places a new emphasis on fraud detection where the auditor would be required to report on the appropriateness and adequacy of systems intended to minimize the risk of fraud.

These proposals highlight the developing format of the EA role that is moving closer to the internal auditor's concerns with the way the company's affairs are managed and controlled. The Cadbury code, which advocated reports by directors and auditors on the systems on internal control, also brings into the frame the concept of management's responsibilities for the overall control arrangements. Again we can see that the growing proximity of internal and external audit pursuits is evident, which calls for more urgency in developing the policies for good cooperation. This also calls for a better distinction of the two functions so that common interests are dealt with in an appropriate fashion and do not lead to a confusion of roles and responsibilities. Meanwhile the APB published the Auditor's Code in 1995, which is not mandatory but members are encouraged to comply with. The code includes:

- **Accountability:** Auditors act in the interest of primary stakeholders, whilst having regard to the wider public interest. The identity of primary stakeholders is determined by references to the statute or agreement requiring an audit: in the case of companies, the primary stakeholder is the general body of shareholders.
- **Integrity:** Auditors act with integrity, fulfilling their responsibilities with honesty, fairness and truthfulness. Confidential information obtained during the course of the audit is disclosed only when required in the public interest or by operation of law.
- **Objectivity and independence:** Auditors are objective. They express opinions independently of the entity and its directors.

- **Competence:** Auditors act with professional skill derived from their qualification, training and practical experience. This demands an understanding of financial reporting and business issues, together with expertise in accumulating and assessing the evidence necessary to form an opinion.
- **Rigour:** Auditors approach their work with thoroughness and with an attitude of professional scepticism. They assess critically the information and explanations obtained in the course of their work and such additional evidence as they consider necessary for the purposes of their audit.
- **Judgement:** Auditors apply professional judgement taking account of materiality in the context of matters on which they are reporting.
- **Clear communication:** Auditors' reports contain clear expressions of opinion and set out information necessary for a proper understanding of that opinion.
- **Association:** Auditors allow their reports to be included in documents containing other information only if they consider that the additional information is not in conflict with the matters covered by their report and they have no cause to believe it to be misleading.
- **Providing value:** Auditors add to the reliability and quality of financial reporting; they provide directors and officers constructive observations arising from the audit process; and thereby contribute to the effective operation of the business, capital markets and the public sector.[120]

Things have moved on and like all business professionals, EA has been swept up into the *risk tide*. The ICAEW Audit and Assurance Faculty has a clear view on this:

> The external audit approach has moved from 'audit risk' to 'business risk' – that is the business risks that the client faces in areas such as business environment, operations and control processes – and auditors spend more time in considering the broader aspects of risks as well as the related management controls. Move from audit to business assurance service[121]

HM Treasury

Guidance issued by the British Government's Treasury covers cooperation between IA and EA. The guide lists benefits, measuring the cooperation and ways of promoting such cooperation and a brief summary follows:

1. **Benefits:**
   - More effective audit based on better understanding of roles.
   - Reduced audit burden.
   - Better informed dialogue on risks facing the organization leading to more effective focusing of audit effort . . .
   - Better coordinated internal audit and EA activity . . .
   - A better understanding by each group of the results arising from each other's work which may inform respective future work plans and programmes.
   - Increased scope for use by both internal and external auditors of each other's work.
   - The opportunity for each party to draw on a wider and more flexible skills base.
2. **Measures:**
   - Commitment – from both parties as an attitude of mind.
   - Consultation – through the audit committee.
   - Communication – two way process, regular meetings again through the audit committee.
   - Confidence – mutual between both groups, both have professional standards and information exchanges are treated professionally and with integrity.

3. **Co-operation:**
   - Internal Control – appropriate measure of risk assessment should be in place.
   - Corporate Governance – internal audit assurances to the accounting officer and external audit should review the statement.
   - Reporting on financial statements – external audit place reliance on internal audit.
   - Compliance with laws and Regs – internal audit activity relevant to EA consideration of propriety.
   - Fraud and Corruption – EA consider the work of internal audit when considering the risks and any bearing on the financial statements.
   - Performance indicators (PI) – internal audit may look at as part of the audit and EA may report on the PIs' outturns.
   - Developing systems/major initiatives – e.g. resource accounting and budgeting.
   - Testing programmes – interrogations.
   - Dispersed organisations – internal audit may visit or work in joint teams.
   - Value for money (VFM) – EA may consider internal audit work when performing a VFM study.
   - Communications with audit committee – e.g. audit adjustments, how accounting estimates arrived at, clarity of disclosures, items with significant impact on the accounts.

Financial Reporting and Independence

The final accounts that are prepared by limited companies represent the main vehicle through which the company communicates with the outside world. The importance of an effective dialogue between corporate bodies and external stakeholders has become a key concern in the business community and there is a growing interest in seeking to improve this communication. One development has been the use of an operational and financial review of the business. Brian Rutherford has considered this practice:

> Operational and Financial Review – narrative reports are more than PR but a way of communicating with less financially literate users or matters than cannot be expressed solely in figures – but these unaudited assertions are viewed with some suspicion. Ways to increase users' confidence in narrative statements:
>
> - build up a record through time for openness, honesty and straight talking.
> - consistency in the pattern of disclosure including revealing bad news.
> - keying the narratives in the published accounts into the annual reporting cycle.
> - an audit review of factual claims and consistency with the financial statements and other audited material.
> - cover business risks, corp gov and future prospects – the company's business model can be an important route to better understanding – model sets out business operations and structure and how strategy is being achieved. Akin to corporate strategy.
>
> Narrative moves away from footnotes into getting the real story told – part of the current review of company law.[122]

This is fine in practice but where the company has misrepresented its financial position there can be tremendous implications for banks, shareholders, suppliers, customers, the tax authorities, its auditors, investment advisors, insurance companies, employees, regulators, managers and all those other stakeholders who are affected by the activities of big corporations. The WorldCom and

Enron examples show the fallout where the misstatements hit the billions mark. In economies where large, short-term returns are expected as the norm and huge bonuses and share options depend on income figures, then all pressures focus on performance targets and financial results. Complex technical conjuring tricks can be used to achieve the right results and stay within the rules, or to achieve the right results and 'appear' to stay within the rules. This is where the EA comes into play – to independently check that what appears to be true is in fact true. This task becomes increasingly difficult where the control environment is poor and the following factors are involved:

- Performance targets are extremely challenging.
- The environment throws up unexpected developments.
- Executives have an aggressive approach to earnings management.
- There is high turnover of technical personnel, particularly in accounting and financial management.
- There is an abundance of complicated intercompany transfers and schemes and third party transactions.
- The board is dominated by a small in-group revolving around the CEO and CFO. The appointed chair has no authority (or inclination) to redress this imbalance.
- Recruitment of senior people is based on personal recommendation.
- The board adopt a high-risk strategy without checking with the auditors.
- One main criterion for new projects is that they are passed by an army of corporate lawyers.
- There are many adjustments and journal transfers made in the accounts and directors are able to override the financial procedures with little documentation.
- The audit committee has little or no financial expertise and has a history of rubber stamping key decisions.
- The control environment and ethical climate encourages a disregard for regulators, auditors and stakeholders. There is little open communication between the board and with managers and employees.
- There is a blame culture in place as well as a 'no bad news' attitude where failure to meet targets is generally unacceptable.
- The staff disciplinary code stresses loyalty to the company and to the management and whistleblowing is not encouraged at all. Here many of what would be considered *red flags* are simply ignored by everyone.
- Where there are poor financial controls and an ineffectual IA function this means transactions can be posted with no real probability of detection.
- And finally – the external auditors are given large amounts of extra work and consulting projects. Moreover, where the auditor asked too many questions, they are simply replaced (many company shareholders simply follow the board's recommendations on auditor selection).

A report on the views of George Monbiot, political commentator and author of *Captive State*, *The Corporate Takeover of Britain*, is appropriate here:

> the aftermath of Enron will encourage stakeholders to question more closely what organisations are up to . . . most organisations do not make much effort to supply more than the minimum amount of information laid down by statute . . . 'The strategy of some organisations is to bombard stakeholders with so much information that no one can possibly get through it all, and even if one does, it would still not give a complete and accurate picture of the state of the organisation.'[123]

Meanwhile, Joseph T. Well of the Certified Fraud Examiners has suggested a simple test for the external auditors to secure inside information on wrongdoings:

> Auditors should make it easier for employees to tell what they know by asking two simple but powerful questions of every appropriate person: 'Has anyone you work with asked you to do something you thought was improper or illegal and are you aware, or do you suspect, fraud within this organisation?'[124], 'Suggestions to help prevent future Enrons'.

The real aim of financial reporting is to communicate with the outside world. Kennesaw State University's Corporate Governance Center has prepared 21st Century Governance and Financial Reporting Principles containing an interesting view on financial reporting:

> Reporting Model – This should be developed so that all tangible and intangible resources, risks, and performance of information-age companies can be effectively communicated to financial statement users. Philosophy and Culture – Financial statements and supporting disclosures should reflect economic substance and should be prepared with the goal of maximising informativeness and transparency. A legalistic view of accounting and auditing (e.g., 'can we get away with it anyway?') is not appropriate. Management integrity and a strong control environment are critical to reliable financial reporting.[125]

The external auditor will perform audit tests that provide a reasonable expectation of uncovering fraud that has a material affect on the financial statements, although it is not their prime objective to uncover fraud. This fine balancing act is described by Emile Woolfe and Moria Hindson in *Accountancy Age* magazine:

> When auditors are unwittingly drawn into such a web of deceit and falsehood it can be difficult to assess their culpability. What opportunities existed for discovering the fraud? Can the fact that a high proportion of documents examined were fictitious, and nothing was as it seemed to be, be used as a viable defence? Much will depend in practice on the efficacy of the auditor's assessment of risk, including their knowledge of heavy funding dependency . . . Caparo case – third parties mere assertion of reliance on an accountant's work will not be sufficient to establish a duty of care on the part of the accountant. The claimant must be able to demonstrate that the accountant was aware that his work was being relied on and that he accepted such a duty to the third party investor. Above all, the court would have to find that imposition of such a duty was fair, just and reasonable in the circumstances . . . Blindly performed bulk testing is pointless – risk assessment with no testing is not enough to uncover fraud – risk assessment and small focused testing may be the right balance – in one fraud if the auditors had visited or called the supplier they would have found out it did not exist.[126]

Many problems are caused by differing perceptions by EA and users of financial statements audited by the external auditors. This is commonly known as the 'Expectations gap'. Many users (including institutional and other shareholders) feel that the external auditor has verified the accounts to ensure that they are correct. They expect the auditor to perform a 100% examination of the underlying transactions that go to produce the resultant figures – an unqualified audit opinion meaning that the accounts are reliable and the financial statements show a true and fair view, and that there are no major frauds in the company. The true position is that the external auditor uses samples for testing and the EA can only provide a reasonable expectation that frauds, errors, insolvency, abuse and problems that have a material affect on the accounts may be uncovered. This dilemma is the basis for many of the claims made against the external auditor for negligence

in the performance of their responsibilities. An analysis of the audit involvement in the Maxwell case by the JDS was based on 57 complaints and the areas of deficient work included:

- inadequate respect for, and incompetent performance in compliance with, obligations to the Investment Management Regulatory Organization;
- deficient work in establishing primary audit facts;
- undue acceptance of management representations;
- deficient consideration of the interests of third parties and persons with fiduciary duties;
- lack of robust implementation of a basic sound system of audit;
- deficient partner review and overview.

> . . . It is important for auditors to have good relationships with their clients, but they must always be vigilant and diligent, and all work must be performed objectively with a due degree of scepticism.[127]

The external auditor is expected to display a degree of professional scepticism and react when they discover indicators of fraud and abuse that impact the reliability of the financial accounts. Moreover due regard should be had to professional auditing standards and the external auditor must show that the audit was performed in a professional manner, by competent personnel and in an objective fashion. This final test has come under increasing scrutiny, in particular where the auditor also provides a great deal of additional services and consulting work for the client. The auditor needs to understand the way the board are motivated and the type of control environment that is in place. Risks to the company should be considered hand in hand with risks to the people who rely on the validity of published financial statements. But this degree of scepticism depends, in turn, on a high degree of objectivity by the external auditor who is not motivated by huge amounts of extra consulting work. Work on this topic by Lancaster University has been reported in *Accountancy Age*:

> Research by Lancaster University suggests that the provision of non audit services impairs audit independence, albeit more severely for smaller firms than the Big Five. Professor Peter Pope from Lancaster University – 'It is widely understood companies can and do exploit the flexibility built into GAAP to manage reported earnings. Earnings management can be "good", when used to signal information to the markets. But it can also be used to hide bad news. This creates a demand for monitoring of financial reporting through internal governance mechanisms and the independent external audit . . . The first stage of the research reveals clear evidence confirming UK listed companies manage earnings upwards to meet basic targets . . . it seems some auditors are less likely to challenge aggressive financial reporting when non audit fees are high. This is consistent with, but admittedly not inconclusive proof of, a link between non audit fees and reduced independence . . . Our research . . . suggests internal organisation structures can be developed to avoid erosion of independence in audit work without eliminating non-audit services.'[128]

Commentators have noted the lack of help from Cadbury, Turnbull and others when reviewing corporate governance codes. The external audit concept is a fundamental part of corporate governance arrangements, even though this aspect of independent scrutiny has been around for many years. One press release that does not pull punches goes straight to the point. The company management controls the auditors and the accountability and audit framework that forms the basis of the stewardship model mentioned in Section 2.2 above does not always hold water:

> Strictly speaking shareholders are supposed to appoint the auditors but the reality is that auditors are appointed by management and management deals with any concerns they have.

> The auditors in one sense are supposed to be checking on management, yet they effectively report to management, are paid by management and when other fee work is involved, are particularly beholden to management. Thus a situation can exist where the financial return to an auditing firm from auditing work is low, but the importance to shareholders of independent audit work is vital. In the US, SEC regulator Lynn Turner claims 'The appearance of independence not only matters, it is the oxygen that keeps our profession alive.' Shareholders must believe that the financial statements can be relied on if investor confidence in share markets is to be retained. This dichotomy can cause problems. On the one hand companies may make use of other fee work as a bargaining point to put pressure on auditors to produce a 'true and fair' view in relation to company accounts. On the other hand auditors wishing to retain high value fee work, may be tempted to appease the company and thus compromise the integrity of the audit.[129]

The debate becomes heated where the external auditor assumes the IA role as well. In the US, the SEC has established policies on this matter.

> The CAE should facilitate communications between the internal audit activity, management, audit committee, and external auditors concerning the SEC rules regarding external auditor independence requirements. It is critical for all parties involved to understand and reach agreement concerning application of the SEC rules. Organisations should reach agreement on how to define internal accounting controls, financial systems, financial statements, and operational internal audit services.[130]

In addition, SEC rules state that an audit firm cannot provide more than 40% of an EA client's IA work, measured in hours. The rules do not restrict internal audit services regarding operational internal audit unrelated to accounting controls, financial systems or financial statements. These rules have been overtaken by the Enron saga where the Senate report is recounted in the subsequent Senate report:

> A US Senate committee investigating the collapse of Enron has slammed the energy group's board of directors for allowing disgraced accountants Andersen to provide both internal and external audit services under what the company used to refer to as an 'integrated audit' approach. The Senate Permanent Subcommittee on Investigations, which had been investigating the matter for six months, also concluded that the company's board knew about and could have halted many of the risky accounting practices, conflicts of interest and disguising of debts that led to Enron's demise. The committee looked at over one million pages of subpoenaed documents and interviewed 13 Enron board members . . . The Senate committee took evidence from independent corporate governance experts who 'condemned the very concept of an integrated audit, not only for diluting the outside auditor's independence, but also for reducing the effectiveness of an outside audit by allowing the auditor to audit its own work at the company.'[131]

Some commentators go further and back in 1998 there were calls for much more focus on external auditing work by specialist firms:

> Donald Butcher (President of the UK Shareholders Association) is also concerned that the external auditors face a conflict of interest when they take on non-audit work. 'We believe it should be unlawful for auditors to carry out non-audit work. There will always be a suspicion that audit fees are artificially low to get non-audit work and that these fees, which can be very large, will compromise the audit. Some institutional investors agree with us, to the extent that they believe non-audit work should be restricted.'[132]

External Audit Reports

These reports follow official professional auditing standards and refer to the legal framework within which the organization operates. What follows is an example of a standard private sector external audit report:

> We have audited the group's financial statements for the year ended 31 March 200x which comprises the Profit and Loss Account, Balance Sheet, Cash Flow Statement of Total Recognised Gains and Losses and the related notes 1 to 35. These financial statements have been prepared on the basis of the accounting policies set out therein.
>
> Respective responsibilities of directors and auditors. The directors' responsibilities for preparing the Annual Report and the financial statements in accordance with applicable United Kingdom law and accounting standards are set out in the Statement of Directors' Responsibilities within the Directors' Report. Our responsibility is to audit the financial statement in accordance with relevant legal and regulatory requirements, United Kingdom Auditing Standards and the Listing Rules of the Financial Services Authority. We report to you our opinion as to whether the financial statements give a true and fair view and are properly prepared in accordance with the Companies Act 1985. We also report to you whether if, in our opinion, the Directors' Report is not consistent with the financial statements, if the company has not kept proper accounting records, if we have not received all the information and explanations we require for our audit, or if information specified by law or the Listing Rules regarding directors' remuneration and transactions with the group is not disclosed. We review whether the Corporate Governance Statement reflects the Company's compliance with the seven provisions of the Combined Code specified for our review by the Listing Rules, and we report if it does not. We are not required to consider whether the board's statements on internal control cover all risks and controls, or form an opinion on the effectiveness of the group's corporate governance procedures or its risk and control procedures.
>
> We read other information contained in the Annual Report and consider whether it is consistent with the audited financial statements. This other information comprises the Directors' Report, Chairman's Statement, Operating and Financial Review and Corporate Governance Statement. We consider the implications for our report if we become aware of any apparent misstatements or material inconsistencies with the financial statements. Our responsibilities do not extend to any other information.
>
> Basis of our opinion. We conducted our audit in accordance with the United Kingdom Auditing Standards issued by the Auditing Practices Board. An audit includes examination on a test basis, of evidence relevant to the amounts and disclosures in the financial statements, and of whether the accounting policies are appropriate to the group's circumstances, consistently applied and adequately disclosed.
>
> We planned and performed our audit so as to obtain all the information and explanations which we considered necessary in order to provide us with sufficient evidence to give a reasonable assurance that the financial statements are free from material misstatement, whether caused by fraud, or other irregularity or error. In forming our opinion we also evaluated the overall adequacy of the presentation of information in the financial statements.
>
> Opinion. In our opinion the financial statements give a true and fair view of the state of affairs of the Company and the group as at 31 March 200x and of the profit and loss of the Group for the year then ended and have been properly prepared in accordance with the Companies Act 1985.

National Audit Office (NAO)

Returning to the UK experience, the Exchequer and Audit Departments Act 1866 created the position of Comptroller and Auditor General (C&AG) and an Exchequer and Audit Department. The National Audit Act 1983 resulted in the C&AG becoming an officer of the House of Commons, reporting to Parliament on VFM within government bodies. The C&AG is appointed by the Queen on address jointly proposed by the Prime Minister and the Chair of the Public Accounts Committee (PAC) (and approved by the House of Commons) and is an officer of the House of Commons. The PAC consists of a team of 15 Members of Parliament and is chaired by a member of the opposition. The Government of Wales Act 1988 established the Auditor General for Wales, while the Audit (NI) Order 1987 established the Northern Ireland Audit Office and the Scotland Act 1998 similarly created the Auditor General for Scotland. The NAO (National Audit Office) audits the Metropolitan Police, and is responsible for the audit of the Police Authority for Northern Ireland, although this work is carried out by the NAO on its behalf. The Audit Commission is responsible for the audit of other police authorities in England and Wales. Note that the Accounts Commission has similar responsibilities for Scotland. It is clear the remit of the NAO goes well beyond verifying the financial statements and involved a view of the quality of services provided by government organizations. The NAO has developed a clear set of objectives to drive their progress:

Vision – to help the nation spend wisely

Mission – to promote the highest standards in financial management and reporting, the proper conduct of public business and beneficial change in the provision of public services.

Values – co-operative spirit, integrity, looking outwards, making a difference, open communications, professional excellence, valuing individuals

To assist these aspirations, the NAO has adopted an audit assurance model that addresses:

- Inherent assurance – inherent risk without considering controls that accounts misstated.
- Controls assurance – whether controls will prevent or detect misstatement and the results testing these controls.
- Substantive assurance – from substantive procedures.

The C&AG's reports go to the PAC, which in turn scrutinizes the plans and progress made by the NAO. The PAC responds to these reports with a Treasury minute and can make recommendations to improve services which have experienced major problems. A new approach to planning and performing financial audits was developed by the NAO after the new millennium termed 'Audit 21', with a view to:

- improving the effectiveness of our audit through a better understanding of the business of our clients and the risks they face;
- increasing efficiency through taking the maximum degree of assurance from management controls and analytical procedures;
- adding value for our clients, through recommendations and suggestions on risk and controls;
- creating more rewarding audit for our staff, through a greater exercise of judgement and less routine testing of transactions.

Audit 21 provides a more focused audit process that involves the following steps:

1. understand the business
2. assess material risks
3. design audit procedures
4. perform audit procedure
5. evaluate results
6. product = audit opinion.

The focus is on understanding the business and the risks that the business faces and the way the organization responds to these risks. This is because these risks can lead to material misstatement and they need to be mitigated properly. There is also due recognition of the control environment and a top-down view of control with less emphasis on detailed compliance testing of individual transactions with more attention paid to monitoring activities carried out in the organization. Auditors are strongly encouraged to derive the maximum degree of assurance from the operation of client monitoring and control procedures to reduce these risks by taking a top-down approach to control assurance. Where substantive assurance is needed, the auditor will tend to use analytical review rather than routine testing. As with most EA arrangements, the NAO may prepare a management letter, where appropriate, suggesting improvements in accounting and financial control systems which have been identified during the audit. In terms of auditing the Accounting Officer's Statement of Internal Control, the Treasury have incorporated the NAO's position with their guidance on this matter:

> The NAO's work on internal control will not be sufficient to enable them to express any assurance on whether the audited bodies are effective. In addition, the financial statement audit should not be relied upon to draw to the accounting officer's attention all matters that may be relevant to their consideration of whether or not the system on internal control is effective. Auditors are not expected actively to search for misstatement or inconsistencies, but if they become aware of such a matter they will discuss it with senior management to establish the significance of the lack of proper disclosure.[133]

More recently, the NAO has prepared a guide that is aimed at accountants of entities producing financial statements under International Public Sector Accounting Standards (IPSAS). The guide shows how entities can prepare for the EA of their IPSAS compliant accounts and the 2007 guide suggests that there needs to be a thorough understanding of the entity risks, systems of internal control.

The Audit Commission

The Audit Commission is the other big independent government external auditor and covers local authorities and NHS bodies, in contrast to central government organizations. Like the NAO it also has responsibility to promote improvement in VFM in public services. The Audit Commission produced a new Code of Practice in March 2002 building on the Audit Commission Act 1998 and the Local Government Act 1999 which addressed the statutory responsibilities and powers of appointed auditors. The Audit Commission is responsible for the appointment of auditors (from private firms and its own agency, the district audit) to local government and health authorities and NHS trusts. The Audit Commission is based on the premise that it supports local democracy by helping to ensure that the members and officers of elected local authorities are accountable to the

communities they serve and by providing assurances that public money has been properly spent. The Audit Commission Act 1998 requires the Commission to 'prepare and keep under review, a code of audit practice prescribing the way in which auditors (appointed by the Commission) are to carry out their functions under the act and which embodies what appears to be the best standards, procedures and techniques to be adopted by the auditors'. Paragraph 20 of this code covers the audit framework and states that:

> In planning their audit work, auditors should consider and assess the relevant significant operational and financial risks that apply to the audited body and the arrangements it has put in place to manage these risks. The aim of this exercise is to prepare an audit plan that properly tailors the nature and conduct of audit work to the circumstances of the audited body, so that audit effort is directed to those areas of highest risk.

Paragraph 21 goes on to say:

> In carrying out their assessment of audit risks, the auditors will need to understand the characteristics of the audited body, its responsibilities and the problems it faces, and the state of its corporate governance arrangements. This will involve discussions with key officers and members, and with internal audit.

The type of audit undertaken at the local authority body is dependent on its size. The Audit Commission will undertake a basic, intermediate or full audit depending on the income/expenditure banding it falls within. Using this form of formalized risk assessment, smaller authorities will only attract the basic EA. The Audit Commission have stated that they will place reliance on the work of IA and the extent of the control environment in place, although they will still undertake some detailed work at organizations chosen at random as a deterrence. Using this focus on providing audit resources where appropriate the Audit Commission argue that the structured audit will:

- provide a reasonable, albeit reduced, level of assurance to stakeholders;
- help to promote proper standards of conduct, by strengthening local councils' own governance; and,
- above all, provide proper accountability for public money.

Much of the actual audit work is carried out by district audit on behalf of the Audit Commission, or contracted-out to accounting firms who are equipped to perform this type of work. Note that local authority EA also has a focus on performance measures and the way they are employed to assess and improve services across the country. Over the years the Audit Commission has developed the concept of the managed audit. Here much of the underlying audit work is performed by the in-house internal audit team and they also work closely with the officers and other review functions within the organization. This approach depends on sound financial and budgeting systems, and a track record of good cooperation between management and the external auditors. In the words of the Audit Commission, this allows the responsibilities of the external auditor to be discharged by:

- communicating clearly what is needed from the organization's staff;
- using the work of the audited body;
- working with management;
- making appropriate use of the work of, and cooperating with, internal audit and other internal review functions;

- making appropriate use of the audited body's working papers; and
- improving project management of the audit process.

In a managed audit, the internal and external audit teams work closely together so that the overall picture is fully coordinated. Some argue that they should prepare similar styles of report so as to present a common front. In practice the managed audit theory fails to recognize the different roles of the two types of audit and certainly not the new drive of internal auditing as a high-level assurance and consulting activity. Many practitioners suggest that using IA as spare resources for EA harks back to the bad old days where IA were just low-level checkers. However, adopting a good working relationship with EA and ensuring that the client does not become confused by a lack of role clarity is a suitable aspiration. Public sector auditors argue that they are also forward looking, by identifying lessons to be learnt and by disseminating good practice as well as playing an important role in the adopted corporate governance arrangements. Paul Gosling has reported on the impact of Best Value initiatives in local government:

> Auditors should be happy. From being confined to the back room, influential but largely unseen, they are being thrust into the foreground. Under Best Value, external auditors will become key people with responsibility for triggering government intervention in failing authorities . . . 'Auditors are being used in ways they haven't before.' said a senior Big Five public sector auditor. 'It is fair for auditors to report on the facts of the plans that authorities have, but where auditors are expected to challenge whether authorities should be more ambitious, we are starting to get into territory which is quite grey and potentially beyond the traditional audit function . . . Best value performance plans are a forecast and to subject them to what is called "an independent audit" is perversion of audit. It becomes very subjective and is very different from private sector audit work . . . David Price the CE of District Audit, is confident that DA can fulfil its new role . . . ' The role of the auditor is to ensure the public that this local authority has made proper plans for the discharge of those duties under Best Value – which is a logical extension of the financial stewardship. Personally I don't have any problems with auditors doing this.[134]

The Audit Commission makes reference to the APB in defining what is significant in terms of their EAs:

> The APB defines this concept (materiality and significance) as 'an expression of the relative significance or importance of a particular matter in the context of the financial statements as a whole. A matter is material if its omission would reasonably influence the decisions of an addressee of the auditor's report. Likewise a misstatement is material if it would have a similar influence . . . Materiality is not capable of general mathematical definition as it has both qualitative and quantitative aspects.'[135]

The audit commission must ensure that it has a way of assessing the quality of the service it provides and whether they carry out their work in accordance with the Commission's Code of Audit Practice (the Code). The Commission has out in place an annual quality review process (QRP), the aim of which is to that provide assurance that the Commission's audit suppliers have suitable systems and procedures in place to ensure the quality of work delivered at audited bodies.

Better Public Sector Audit Coordination

The lack of clarity between internal and external audit is nothing compared to the potential for confusion between the various sets of public sector external auditors. The Public Audit Forum

(PAF) addresses standards for all types of public sector external auditors as is based on a joint statement in October 1998 from the NAO, NI Audit Office, Audit Commission and Accounts Commission for Scotland. For the PAF the audit process (including internal audit, is deemed to be based on three principles:

- independence of the public sector auditors – appointment, fees, access, complete discretion on how they exercise their functions;
- wide scope – financial statements, regularity (transactions comply with laws and regs), probity (how business is conducted) and VFM;
- results of audits available to the public.

The PAF have defined the service expected from public auditors:

- integrity and objectivity;
- professionalism;
- openness;
- cost-effectiveness;
- consideration for the auditee – providing guidance, coordinating the audit work, taking auditee concerns into consideration, opinions provided in a fair and constructive manner.

Meanwhile the Sharman review of government audit and accountability sets a new agenda for:

- removing anomalies in the audit arrangements for government;
- further encouraging moves to improve the internal control arrangements within departments.[136]

Corporate Reporting

The WorldCom, Enron and other major cases of financial misreporting have put great pressure on the external audit community to ensure that there is no conflict of interest in the way it furnishes its opinion on the accounts. There is an ongoing review of auditor independence and the issue of non-audit fees and whether they should be further restricted. Rotation of senior audit partners is another measure that should increase independence and there are moves to decrease the time frame for such rotations (currently from seven to five years). Another high profile issue relates to periodic retendering for the external audit contract and whether there should be compulsory rules for such measures. The prime objective is to ensure the external auditor focuses on the final accounts, and has no distractions that impair the external auditor from delivering an objective and challenging review of the final accounts through the adoption of a healthy degree of professional scepticism. We are in a state of continuous review as report after report analyses the rules and practices that promote better auditor independence, or help improve the perceived state of independence of the external audit process. Extracts from an article from Anthony Hilton provide a hint of things to come:

> Trade Secretary Patricia Hewitt will this week announce an investigation into auditors . . . This body will examine what measures can be introduced to ensure the independence of auditors . . . compulsory rotation of auditors being the main idea . . . all auditing scandals in the past 30 years have occurred when a strong CEO has intimidated the auditor or committed fraud, or both . . .

> Meanwhile in America Walt Disney felt the renewed strength of the shareholder movement . . . At Disney's annual general meeting, a surprisingly large number of institutional investors backed a proposal that would have barred Disney from hiring its auditor for other consulting services . . . Politicians and regulators will debate for months the wisdom of separating accounting and consulting but, fittingly, shareholders could turn out to be the biggest catalyst for change.[137]

The Department of Trade and Industry (DTI) review has focused on many related developments on company law, the adoption of international accounting standards, statutory operating and financial review and the role of executives and non-executive directors. The question of NEDs' independence is also a developing issue as is the much vexed matter of increasing external auditor independence. There are calls to strengthen the EA and retain a higher degree of credibility by measures such as:

- Stopping external auditors from providing any non-audit services and promoting the growth of accounting firms that specialize in only providing external audit and no consulting services at all. Note that during 2003, no ban was provided over non-audit fees, although accounting firms were required to make more disclosure of earnings.
- Getting the audit committee to appoint, monitor and terminate the EA using a carefully prepared specification that stresses independence and professionalism. At least one member of the audit committee should be a qualified accountant.
- Retendering the EA contract periodically to instil competition. Although some argue that the incoming auditor will be new and may not be able to cope with complicated financial arrangements.
- Rotation of the senior partner on the audit so that there is less chance of excessive familiarity between the partner and the company executives.
- Better clarification of the role of the external auditor in terms of the degree of reliance that can be placed by users of published financial statements on the audit report.
- Interim audit accounts and audit coverage extended to statements and information released by the company.
- More robust quality assurance regimes with scrutiny from the professional bodies.

When considering the relationship between internal and external audit we must mention issues such as professionalism, the audit image, training, marketing and good relations with EA and others. This is because good relationships do not mean standing in EA's shadow and being used by it as it pleases. It means an equal relationship with professional respect from both sides, which has to be earned before it can be demanded. Relationships with other review agencies should likewise be clearly established since there may be some scope for coordination. IA should seek to ensure that it assumes a higher status in the organization than these other review teams, which should also be subject to IA cover in the normal course of planned audit work. In terms of other review agencies, the IA role within the organization should be firmly established and contrasted with other available services. In addition, an element of competition may lead to the services becoming blurred. This is where a formal audit charter helps define and publicize the audit mission as long as this is supported by a base of professional audit staff. There is also a link into the audit approach and if there are no client-based marketing plans, audit's future may become somewhat insecure.

Some of the more recent annual reports reflect the need to engage more fully with stakeholders and ensure that companies explain their governance process in some detail. Extracts from a small selection of published reports will help clarify this point. We start with extracts from the annual report of John Menzies plc:

The directors are responsible for the Group's system of internal control, which covers financial, operational and compliance controls together with risk management. Whilst no system can provide absolute guarantee and protection against material loss, the system is designed to give the directors reasonable assurance that problems can be identified promptly and remedial action taken as appropriate. The directors, through the board's review of risk and the work of the audit Committee, have reviewed the effectiveness of the system of internal control for the accounting period under review and consider that it accords with revised guidance. There were no material weaknesses in the Group's system of internal control relating to financial control during the year. The key features of the Group's internal control system are:

Control Environment

A key factor in the Group's approach to internal control is the recognition of the need for risk awareness and the ownership of risk management by executives at all levels. Each operating division has its own Board. A Statement of Group Policies and Procedures sets out the responsibilities of these Divisional Boards, including authority levels, reporting disciplines and responsibility for risk management and internal control. Certain activities, including treasury, taxation, insurance, pension and legal matters are controlled centrally with reports reviewed by the Board as appropriate.

Risk Identification and Review

Key identified risks, both financial and non financial (the latter including environmental, social and governance "ESG" risks), are reviewed by the Board as well as at Operating Board level on an ongoing basis, with a formal annual review of risks and controls taking place, supported by the Group's Controls Assurance provider.

The Divisional Operating Boards also review each division's performance, strategy and risk management. Annual compliance statements on internal control are certified by each Divisional Board. A Treasury Review Committee meets regularly to review the adequacy of the Group's facilities against potential utilisation and commitments, as well as to monitor and manage the Group's exposure to interest rate and currency movements.

Key Non-Financial Business Risks

The management of the business and the execution of strategy are subject to a number of risks, beyond those identified in the Group Financial Review in the 2008 Annual Report. Risks are formally reviewed by each Divisional Operating Board on an annual basis. A formal Group-wide review of risks is also performed annually by the Group Board and appropriate processes and controls are put in place to monitor and mitigate these risks.

The key non-financial business risks affecting the Group are as follows:

Safety & Security: This is the risk of safety and security incidents occurring within the business. Both divisions have dedicated teams who regularly visit operational sites, monitoring health and safety and security issues and drive improvements. They also monitor legislative and regulatory changes. We work with industry bodies to lead improvements and to benchmark our performance. Monthly reports are tabled at the Divisional Operating Boards and the Group Board.

Changing business environment: This is the risk that we do not respond to a changing business environment. Following stability in the market environment in 2007 for both Menzies Aviation and Menzies Distribution, 2008 saw a far more challenging year for Menzies Aviation. A strategy review exercise, which involves a full examination of market conditions, is held each year prior to budget setting. Board reports from each Managing Director, reviewing all aspects of market conditions, are tabled for discussion at each meeting. Customer surveys have been introduced in both divisions which we will repeat regularly.

Investment decisions: This is the risk of making the wrong corporate portfolio investment decisions. An investment review committee exists which meets whenever it is required to review significant capital expenditure decisions and all acquisitions and disposals. Projects are measured against a number of strict financial criteria such as payback, net present value and internal rate of return. Recommendations from the investment review meetings must be ratified by the Group Board. All potential acquisitions are subject to rigorous due diligence involving internal and external specialists.

People development: This is the risk that we do not successfully develop our people and lose key management. To mitigate this risk, the Group has introduced a leadership development programme and a regular 360 degree appraisal process. A number of incentive schemes linked to the Group's results have been designed to help retain key managers.

External shock: This is the risk of the business being impacted by a major external shock, such as terrorism, disease, or natural disaster. To mitigate this risk, we have emergency response procedures in place at both divisions, which deal with communication guidelines, customer liaison, staff safety contingency actions and escalation procedures. In each division, we have developed strong leadership teams with a broad experience of dealing with a wide variety of operational issues.[138]

The next annual report from Transport for London, gives the public sector view of corporate governance:

Statement of Corporate Governance Assurance

Scope of responsibility The Statement of Corporate Governance Assurance reports on the current standard of corporate governance, including internal control, within Transport for London (TfL). It identifies those areas where further work is to be undertaken and gives a brief description of the monitoring process to ensure the effectiveness of the Code of Corporate Governance.

TfL is responsible for ensuring that its business is conducted in accordance with the law and proper standards, and that public money is safeguarded and properly accounted for, and used economically, efficiently and effectively.

TfL also has a duty under the Local Government Act 1999 to make arrangements to secure continuous improvement in the way in which its functions are exercised having regard to a combination of economy, efficiency and effectiveness. In discharging this accountability, Board members and senior managers are responsible for putting in place proper arrangements for the governance of TfL's affairs and the stewardship of the resources at its disposal, including arrangements for the management of risk.

To this end, TfL has approved and adopted a Code of Corporate Governance, which is consistent with the principles and reflects the requirements of the CIPFA/SOLACE framework and the requirements of the Accounts and Audit Regulations 2003.

Purpose of the system of corporate governance assurance TfL has put in place appropriate management and reporting arrangements to enable it to satisfy itself that its approach to corporate governance is both adequate and effective in practice. Specifically, it has an established system of internal control. This is designed to manage risk to a reasonable level rather than to eliminate all risk of failure to achieve policies, aims and objectives; it can therefore only provide reasonable and not absolute assurance of effectiveness. The system of internal control is based on an ongoing process designed to identify and prioritise the risks to the achievement of TfL's policies, aims and objectives, to evaluate the likelihood of those risks being realised and the impact should they be realised, and to manage them efficiently, effectively and economically.

Corporate governance in TfL Corporate governance is the system used to direct, manage and monitor an organisation and enable it to relate to its external environment. The fundamental principles of corporate governance, to which TfL is fully committed are openness, inclusivity, integrity and accountability.

Using the nationally recognised CIPFA/SOLACE framework, TfL developed and published a Code of Corporate Governance in 2002 tailored to its own circumstances, which is designed to make its adopted practices in this area open and explicit.

On an annual basis, TfL agreed to undertake a wide-ranging review of its relevant activities involving all senior managers to determine the degree to which TfL's methodologies conform to the Code's requirements. Where they have been found wanting, action plans are being developed to identify and implement remedial action.[139]

The governance statement from a listed company is set out below:

> The Board of directors of the Company is committed to maintaining high standards of corporate governance and to managing the affairs of the Group in accordance with the provisions of the Listing Rules and of the Combined Code on Corporate Governance, issued by the Financial Reporting Council in June 2008 (the "Combined Code"). A copy of the Combined Code is available on the Financial Reporting Council's website at www.frc.org.uk. The Board has reviewed the Company's corporate governance processes and policies, and has concluded that during the 52 weeks ended 26 April 2009 (the "Year") the Company complied with the provisions of the Combined Code except as set out below.
>
> The Combined Code (code provision A3.2) recommends that at least half of the Board of directors of a UK listed company, excluding the Chairman, should be comprised of non-executive directors determined by the Board to be independent in character and judgement and free from relationships or circumstances which may affect, or could appear to affect, the director's judgment. During the Year the Board was made up of the Acting Chairman, three executive directors and two independent non-executive directors. Accordingly during the Year the Company did not comply with this provision of the Combined Code in this regard.
>
> The Combined Code also provides (code provisions B2.1 and C3.1) that each of the Remuneration and Audit Committees of the Board should comprise of at least three independent non-executive directors. The Code also provides that, in respect of the Remuneration Committee, the Company Chairman may also be a member, but not chair, the Committee if he or she was considered independent on appointment as Chairman. During the Year these committees comprised two independent non executive directors and the Acting Chairman.

Accordingly during the Year the Company did not comply with these provisions of the Combined Code.

The Combined Code provides (code provision A.4.1) that the majority of the members of the Nomination Committee should be independent non-executive directors. During the Year the Committee comprised the Acting Chairman, the Executive Deputy Chairman and two non-executive directors. Accordingly during the Year the Company did not comply with this provision of the Combined Code. Since the end of the Year Mike Ashley has ceased to be a member of the Nomination Committee, and the structure of this Committee is now compliant with the provisions of the Combined Code.

The Company has in the past used recruitment consultants to search for a Chairman and for additional independent non-executive directors and the Nomination Committee has approved job descriptions for those roles, which for the Chairman includes an assessment of the time commitment expected, always recognising the need for availability in the event of major activity.

The Board currently believes, however, that the Board and its committees as currently constituted are working well, and that in a period of challenging economic conditions it would be difficult to recruit an appropriate person to be either the Chairman or an independent non executive director of the Company.

Accordingly, while the Board intends when practicable to appoint a further independent non-executive director to the Board and to both of the Remuneration and Audit committees, which would bring the Company into compliance with all the provisions of the Combined Code, no steps are currently being taken to achieve that. The Nomination Committee and the Board will, however, keep the position under review.[140]

Extracts from another governance statement follows:

The HSA Board and Senior Management Team are committed to maintain a high standard of corporate governance and advocate the recommendations set out by the Code of Corporate Governance. The Board believes that good governance is essential in enhancing corporate performance and accountability, ensuring transparency and protecting stakeholders' interests at all times. Our stakeholders include the Ministry of Health, Ministry of Finance, other government agencies, the healthcare industry, our clients, our suppliers and the public at large.

This statement outlines the main corporate governance practices of the organisation that are in place.

The Board

The Board comprises the Chairman and its members, who are appointed by the Minister for Health for a 3-year term. It aims to meet every two months to set strategic directions and formulate policies, assuming the role of monitoring and reviewing of policies leading to HSA's improved management and performance.

Board Members' Remuneration

HSA follows the Government's Directorship and Consultancy Appointments Council (DCAC) guidelines in determining the remuneration of the Board Members.

Notice and Declaration of Directorships and Interest in Shares and Debentures

Board Members are required to declare their directorships in various organisations and their interests in shares and debentures in various corporations. Board Members deemed to be interested in any such transactions made during the meetings are reminded and required to declare their interest; they are to refrain from any deliberation made when such an interest has been declared.

Accountability and Audit

HSA's Senior Management Team is accountable to the Board. In return, the Board is accountable to the Minister for Health. To allow the Board to discharge their duties adequately, Senior Management and staff are required to provide periodic updates and answer any queries that the Board may have on the operations and planning of the organisation.

For Accountability purposes, the Board has established the following sub-committees:

(a) The Audit Committee

This Committee assists the Board to review and assess the adequacy of internal accounting controls and financial reporting controls. It meets at least twice a year with the Management and auditors to determine the scope of the external and internal audit and to review the findings of its appointed auditors.

(b) The Staff Establishment Committee

The Staff Establishment Committee assists the Board in reviewing the adequacy of manpower numbers and budgets to meet operational needs and major Human Resource Policies regarding compensation. It oversees some staff matters such as the appointment of senior management positions.

(c) The Finance Committee

This Committee assists the Board in ensuring that financial resources are managed and utilised prudently and in the most effective and efficient manner, contributing towards the organisation's overall mission.

Communication with Stakeholders

The professional groups conduct regular consultations with the industry and their clients, seeking to keep them informed of new directions and regulations, and to listen to their concerns. HSA publishes an annual report to meet statutory requirements and to provide information to our stakeholders.

In addition, regular updates on matters of interest to our stakeholders are posted on our Internet website. Our Quality Service Manager promptly handles all feedback and queries received from interested parties.

Code of Business Conduct

The Board, officers and employees are required to observe and maintain high standards of integrity, and are in compliance with the law and government regulations, and organisation policies.

Risk Management

The Management is continually reviewing and improving the business and operational activities to identify areas of significant business risks as well as appropriate measures to control and mitigate these risks. The Management also reviews all significant control policies and procedures and highlights all significant matters to the Board and the Audit Committee[141]

Sainsbury's is a large retail company and extracts from their corporate governance statements are set out below:

Internal control

The Board has overall responsibility for the system of internal controls, including risk management, and has delegated responsibility for reviewing its effectiveness to the Audit Committee. The system of internal controls is designed to manage rather than eliminate the risk of failure to achieve the Company's business objectives and can only provide reasonable and not absolute assurance against material misstatement or loss. It includes all controls including financial, operational and compliance controls and risk management. The processes used to assess the effectiveness of the internal control systems are ongoing, enabling a cumulative assessment to be made, and include the following:

- discussion and approval by the Board of the Company's strategic direction, plans and objectives and the risks to achieving them;
- review and approval by the Board of budgets and forecasts, including both revenue and capital expenditure;
- regular operational and financial reviews of performance against budgets and forecasts by management and the Board;
- regular reviews by management and the Audit Committee of the scope and results of internal audit work across the Company. The scope of the work covers all key activities of the Group and concentrates on higher risk areas;
- reviews of the scope of the work of the external auditors by the Audit Committee and any significant issues arising;
- reviews by the Audit Committee of accounting policies; and
- consideration by the Board of the major risks facing the Group and by the Audit Committee of the procedures to manage them. These include health and safety, legal compliance, litigation, quality assurance, insurance and security and social, ethical and environmental risks.

There is an ongoing process for identifying, evaluating and managing the significant risks faced by the Company. This process has been in place throughout the year under review and up to the

date of approval of the Annual Report and Financial Statements and accords with the Turnbull guidance. The effectiveness of the process is reviewed annually by the Audit Committee which then reports to the Board. The process consists of:

- formal identification by management at each level of the Company through a self assessment process of the key risks to achieving their business objectives and the controls in place to manage them. The likelihood and potential impact of each risk is evaluated;
- certification by management that they are responsible for managing the risks to their business objectives and that the internal controls are such that they provide reasonable but not absolute assurance that the risks in their areas of responsibility are appropriately identified, evaluated and managed;
- reporting and review by the board of each operating company of risk management activities and actions taken to address non-compliance with controls or to improve their effectiveness;
- assurance from specialist functions and committees that legal and regulatory, health and safety, and social, ethical and environmental risks are appropriately identified and managed; and
- independent assurance by Internal Audit as to the existence and effectiveness of the risk management activities described by management.

The system of internal control and risk management is embedded into the operations of the Company, and the actions taken to mitigate any weaknesses are carefully monitored.[142]

British American Tobacco p.l.c. prepared corporate governance statements as part of their 2008 annual report.

Internal control

The Board is responsible for the overall system of internal control for the Company and its subsidiaries, and for reviewing the system's effectiveness. With the support of the Audit Committee, it carries out such a review annually, covering all material controls including financial, operational and compliance controls and risk management systems, and reports to shareholders that it has done so.

Overview

The Company maintains a sound system of internal control with a view to safeguarding shareholders' investment and the Company's assets. It is designed to identify, evaluate and manage risks that may impede the achievement of the Company's business objectives rather than to eliminate these risks and can therefore provide only reasonable, not absolute, assurance against material misstatement or loss. A description of the key risk factors that may affect the Group's business is provided in the Business review.

The main features of the risk management processes and system of internal control operated within the Group are identified below. They do not cover the Group's associate undertakings. Save to the extent indicated (in relation to developments which occurred during the year), they have been in place throughout the year under review and remain in place.

Audit and CSR Committee framework

During 2008, the Group's Audit Committee and CSR Committee networks were merged at regional level and (where possible) at area and individual market levels, on the basis that many of the issues being considered by them at regional level and below were similar or related (for example, financial and reputational risk factors). The Audit and CSR Committee framework supports the Board's Audit and CSR Committees and provides a continuing process for managing the significant risks faced by the Company and its subsidiaries, including not only financial risks but also significant social, environmental and reputational risks. It is designed to capture and evaluate failings and weaknesses and to ensure that appropriate remedial action is taken where necessary.

The Group's regional audit and CSR committees (which are all chaired by an Executive Director) focus on risks and the control environment within each region and are in turn supported by area and/or individual market audit and CSR committees. The Group's corporate audit committee focuses on the risks and the control environment within the Group's operations which do not fall under the responsibility of the regional, area and local audit and CSR committees, for example head office central functions, global programmes and above-region projects. It comprises members of the Management Board and is chaired by a Management Board member responsible for 1 of the Group's regions to maximise its independence from central executive management.

The relevant external and internal auditors regularly attend meetings of these committees and have private audiences with members of the committees at least once each year. In addition, central, regional and individual market management, along with internal audit, supports the Board in its role of ensuring a sound control environment.

Risk management and internal control processes

Risk registers are used at Group, regional, area and individual market level to identify, assess and monitor the key risks (both financial and non-financial) faced by the business at each level. Mitigation plans are required to be in place to manage the risks identified and the risk registers and mitigation plans are reviewed and, where appropriate, updated on a regular basis. They are also reviewed regularly by the relevant audit and CSR committee, the corporate audit committee or, in the case of the Group risk register, by the Board's Audit Committee.

Group companies and other business units are required at least annually to complete a checklist of the key controls which they are expected to have in place, called Control Navigator. Its purpose is to enable them to self-assess their internal control environment, assist them in identifying any controls which may require strengthening and support them in implementing and monitoring action plans to address control weaknesses. In addition, at each year end, Group companies and other business units are required to:

- review their system of internal control, confirm whether it remains effective and report on any material weaknesses and the action being taken to address them; and
- review and confirm compliance with the Standards of Business Conduct and identify any material instances of non-compliance or conflicts of interest identified.

The results of these reviews are reported to the relevant regional audit and CSR committee or to the corporate audit committee and, where appropriate, to the Board's Audit Committee to ensure that appropriate remedial action has been, or will be, taken where necessary.

The Group's internal audit function provides advice and guidance to the Group's businesses on best practice in risk management and control systems. It is also responsible for carrying out audit checks on Group companies and other business units, and does so against an audit plan presented annually to the Audit Committee, which focuses in particular on higher risk areas of the Group's business.

Review

The Turnbull Guidance (the Guidance) sets out best practice on internal control for UK-listed companies to assist them in assessing the application of the Code's principles and compliance with the Code's provisions with regard to internal control. The current version of the Guidance applies to listed companies for financial years beginning on or after 1 January 2006.

The processes described above, and the reports that they give rise to, enable the Board and the Audit Committee to monitor the internal control framework on a continuing basis throughout the year and to review its effectiveness at the year end. The Board, with advice from its Audit Committee, has completed its annual review of the effectiveness of the system of internal control for the period since 1 January 2008. No significant failings or weaknesses were identified and the Board is satisfied that, where specific areas for improvement have been identified, processes are in place to ensure that the necessary remedial action is taken and that progress is monitored. The Board is satisfied that the system of internal control is in accordance with the Guidance.[143]

2.7 The Audit Committee

The topic of audit committees has an interesting background. The audit committee (AC) is a standing committee of the main board and tends to consist of a minimum of three NEDs. Most audit committees meet quarterly and they are now found in all business and government sectors for larger organizations. The format is normally that the NEDs sit on the audit committee and the CFO, external audit, CEO and CAE attend whenever required. The committee will have delegated authority to act in accordance with its set terms of reference and also investigate areas that again fit with their agenda. The CAE will present reports to most regular committee meetings and will prepare an annual report to cover each financial year in question. This simple format hides many complicated and fundamental issues that cause many difficulties. In short, the audit committee is increasingly seen as one of the cornerstones of corporate governance. Many argue that the success of an organization's corporate governance arrangements relies in part on the success of the established audit committee. Failings in the membership, format, role, competence and commitment of this forum blast a hole in the organization's defined system of corporate governance. The Special Committee of Enron Corp.'s Board of Directors report stated that: 'The Board assigned the Audit and Compliance Committee an expanded duty to review the transactions, but the committee carried out the reviews only in a cursory way. The board of directors was denied important information that might have led them to take action.' We would hope that the audit committee is now providing another layer of stakeholder comfort in the search for good corporate governance and allows us to add to our growing model in Figure 2.8.

Groundbreaking work was performed in the US by the Blue Ribbon Committee in 1998 who prepared ten key recommendations on improving the effectiveness of ACs:

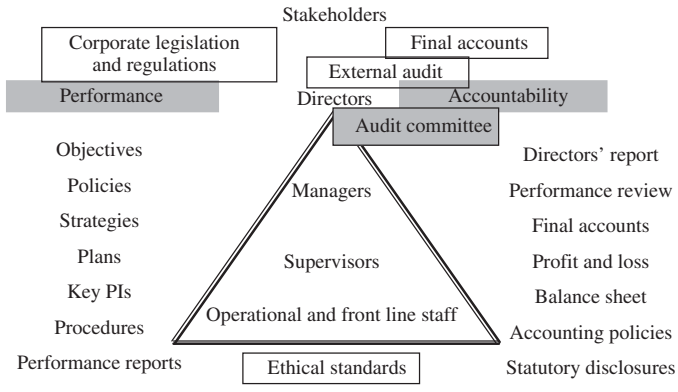


FIGURE 2.8 Corporate governance (5).

1. NYSE and NASD adopt a definition of independent directors – not employed by (last 5 years) associate, family contact, partner, consultant, executive on company whose executives serve on the Remuneration committee etc. No relationship with the company that will impair independence.
2. NYSE and NASD listed companies with market capitalization over $200m have an AC of only NEDs.
3. NYSE and NASD listed companies with market capitalization over $200m have an AC minimum of 3 directors each of whom is financially literate and at least one member has accounting or related financial management expertise.
4. NYSE and NASD listed companies have an AC charter reviewed annually. Details of the charter disclosed in the companies proxy statement to annual shareholders' meeting.
5. SEC rules – statement that AC has satisfied its responsibilities under its charter.
6. NYSE and NASD charters of listed companies specify that external audit is accountable to the board and AC who have the ultimate authority to select, evaluate and replace the external auditor.
7. NYSE and NASD AC charter requires that the AC receive a formal statement detailing relationship between external audit and company, the AC should discuss EA independence and take or recommend to the board action to ensure independence of the external auditor.
8. GAAP revised to require external audit to discuss the auditor's judgement about the quality of accounting principles and financial reporting with the AC.
9. SEC adopt rules that the AC make a Form 10-K Annual Report covering: management has discussed quality of accounting principles, discussions with EA, discussed by AC members, AC believes financial statements are fairly presented and conform with GAAP.
10. SEC adopt rules that external audit conduct a SAS 71 Interim Financial Review before filing Form 10-Q and discuss the financial statements with the AC before filing the Form.

Staying with the US, each audit committee for companies listed on the NYSE, Nasdaq and AMEX must have a charter that shows:

- The scope of the AC responsibilities and how it carries them out.
- Ultimate accountability of the independent auditor to the board and AC.
- Ultimate authority of the board and AC to select, evaluate, and replace the independent auditors.
- The AC responsibilities regarding the independent auditor's independence.

The role of the audit committee is now firmly entrenched in business culture and they are mandatory for most international stock exchanges including London and New York. Even in smaller companies, their presence is recommended by many businesses – which some see as a substitute for an internal audit function.

The Role of the Audit Committee

An audit committee will be established by the main board to perform those duties that the board decides should be properly allocated to this specialist forum. There has been a long fight to get the audit committee accepted by all as there was a view that the audit committee would blur the lines between boardroom executives' responsibilities and the interventions made by non-executives who may have poor understanding of the business. The absence of good NEDs was another reason behind the slow growth of this type of business forum. The new look audit committee has several distinct features, but will have a format that suits the organization in question, which means each audit committee will be completely different and there is no set standard that may be employed to define the role. We have already suggested that a 'one size fits all' approach to corporate governance structures is unrealistic, which is why most codes are both voluntary and fairly general in the way they define set standards. There is still scope to prepare best practice guides, even though they cannot be too specific. The Financial Reporting Council has set out how the audit committee fits in with good governance in their combined code on corporate governance:

C.3 Audit Committee and Auditors
Main Principle The board should establish formal and transparent arrangements for considering how they should apply the financial reporting and internal control principles and for maintaining an appropriate relationship with the company's auditors.

Code provisions
C.3.1 The board should establish an audit committee of at least three, or in the case of smaller companies two, independent non-executive directors. In smaller companies the company chairman may be a member of, but not chair, the committee in addition to the independent non-executive directors, provided he or she was considered independent on appointment as chairman. The board should satisfy itself that at least one member of the audit committee has recent and relevant financial experience.

C.3.2 The main role and responsibilities of the audit committee should be set out in written terms of reference and should include:

- to monitor the integrity of the financial statements of the company, and any formal announcements relating to the company's financial performance, reviewing significant financial reporting judgements contained in them;
- to review the company's internal financial controls and, unless expressly addressed by a separate board risk committee composed of independent directors, or by the board itself, to review the company's internal control and risk management systems;
- to monitor and review the effectiveness of the company's internal audit function;
- to make recommendations to the board, for it to put to the shareholders for their approval in general meeting, in relation to the appointment, reappointment and removal of the external auditor and to approve the remuneration and terms of engagement of the external auditor;

- to review and monitor the external auditor's independence and objectivity and the effectiveness of the audit process, taking into consideration relevant UK professional and regulatory requirements;
- to develop and implement policy on the engagement of the external auditor to supply non-audit services, taking into account relevant ethical guidance regarding the provision of non-audit services by the external audit firm; and to report to the board, identifying any matters in respect of which it considers that action or improvement is needed and making recommendations as to the steps to be taken.

C.3.3 The terms of reference of the audit committee, including its role and the authority delegated to it by the board, should be made available. A separate section of the annual report should describe the work of the committee in discharging those responsibilities.

C.3.4 The audit committee should review arrangements by which staff of the company may, in confidence, raise concerns about possible improprieties in matters of financial reporting or other matters. The audit committee's objective should be to ensure that arrangements are in place for the proportionate and independent investigation of such matter and for appropriate follow-up action.

C.3.5 The audit committee should monitor and review the effectiveness of the internal audit activities. Where there is no internal audit function, the audit committee should consider annually whether there is a need for an internal audit function and make a recommendation to the board, and the reasons for the absence of such a function should be explained in the relevant section of the annual report.

C.3.6 The audit committee should have primary responsibility for making a recommendation on the appointment, reappointment and removal of the external auditors. If the board does not accept the audit committee's recommendation, it should include in the annual report, and in any papers recommending appointment or reappointment, a statement from the audit committee explaining the recommendation and should set out reasons why the board has taken a different position.

C.3.7 The annual report should explain to shareholders how, if the auditor provides non-audit services, auditor objectivity and independence is safeguarded.[144]

The role of the audit committee may therefore incorporate some of the following components in its terms of reference:

1. The external audit process To review the EA process and make recommendations to the board where appropriate, in the following areas:

- Appointment, fees and retention of the external auditor based on an evaluation of performance.
- Review the engagement letter and any special terms and conditions contained therein.
- Consider and agree external audit's plans and the way the work is scheduled throughout the year and after the year end.
- Ensure that EA completes all aspects of the audit plan.
- Ensure that the external auditor is independent and that all matters that impair this independence are properly addressed.

- Ensure all concerns raised by the external auditor are dealt with by company management.
- Ensure that the external auditor has a healthy relationship with company officials and that they are able to perform the audit in a professional manner.
- Review non-audit fees and assess whether they impact on the independence of the EA process. It may be necessary to compile criteria for non-audit fees and have the AC recommend what extra consulting work should or should not be commissioned.

2. The final accounts To consider the annual accounts and the EA report that attaches to these accounts:

- Discuss the accounts with senior management where appropriate.
- Ensure that any concerns regarding the accounts raised by the external or internal auditors are properly addressed.
- Recommend that the board approve the final accounts.
- Consider the accounting policies used and assess areas where discretion is applied to material and complex arrangements. Also consider where accounting policies are unusual or different from the previous accounting period.
- Assess the extent to which the annual report gives shareholders and other users the information they need in the form they require.
- Consider whether there is scope for financial misreporting.

3. Systems of internal control To consider the adequacy of systems of internal controls. The current move to require directors to report on their systems of internal control means that this is starting to assume a higher profile:

- Consult with the external and internal auditor to secure a view on the adequacy of the firm's internal controls.
- Review auditor's material recommendations for improvements to internal control and management's response.
- Special reports on breach of internal control and abuse of corporate assets.
- Review significant related party transactions that affect the accounts.
- Review the external auditor's management letter on internal controls.
- Review the overall control environment within the organization and whether the right messages are being sent from senior management, and that these messages match and set standards for the working practices adopted.
- Assess if there is an agreed control framework in use and that this framework promotes good control over areas where there are unacceptable risks.

Furthermore, Andrew Chamber's *Corporate Governance Handbook* contains a number of inputs in its consideration of the organization's internal controls:

- Intelligence gathered as board members during the year.
- Confirmation that key line managers are clear about their objectives.
- A report from the Executive on key risks.
- A report from the Executive on the key procedures which are designed to provide effective internal control. E.g. – the audit committee itself, a code of business conduct, the budgetary control system, a formal process of risk assessment, internal audit, a credit committee, and control risk self assessment (CRSA)
- The committee's assessment of the effectiveness of internal audit.

- Reports from internal audit on scheduled audits performed.
- Reports on special reviews commissioned by the committee from internal audit or others.
- Internal audit's overall summary opinion on internal control . . . usually it will be unacceptable for this opinion to be qualified by protestations about inadequate internal audit resources and coverage – the audit committee itself will not wish to qualify its opinion on internal control in these ways.
- The overall results of a control self-assessment process.
- Letters of representation ('comfort letters') on internal control from line management.
- The external auditor's management letter.
- A losses report from the CEO or Finance Director (FD).
- An executive report on any material developments since the balance sheet date and the present.
- The Executive's proposed wording of the internal control report for publication.

4. Internal audit Involvement in the appointment of the internal auditors and ensuring that the IA function operates to professional standards, performs well and discharges its responsibilities under the audit plan and strategy:

- Review the IA objective and mission statement and ensure that this provides the platform for a value-added and risk-based audit strategy. The objectives should be set within a formally adopted audit charter.
- Oversee IA activities and organization.
- Agree the IA strategy and annual audit plan – and changes made during the year.
- Discuss the adequacy of the internal controls with internal auditor and management where appropriate.
- Consider any legal matters that impact on the company.
- Meet in private with the CAE and be open to any concerns and issues raised by this officer.
- Review the overall performance of IA and receive (and act on) regular reports from the CAE on progress made in achieving defined key performance indicators.
- Ensure that the IA service works to professional standards and has a robust quality assurance system in place.
- Consider reports from external reviews of internal auditing, including surveys from audit clients across the organization.
- Agree the criteria established by IA to assess the type of consulting projects that it will respond to and review the results of these projects and whether they add value to the organization.
- Receive the annual internal report and presentation from the CAE and insist on a formal opinion of the adequacy of internal control within the organization.
- Ensure there is good communication between the internal auditors, external auditors, board and management – which promotes the achievement of IA objectives.

Again, the *Corporate Governance Handbook* suggests several specific tests that the AC should make as part of its oversight responsibility for IA:

- Is the complement of internal auditors sufficient?
- Are the experience and qualifications of the internal auditors appropriate?
- Is the scope of internal audit unrestricted?
- Is internal audit sufficiently independent of management?
- Is the charter of the internal auditing function appropriate?
- Is internal auditing conducted with due professionalism?

- What is the level of acceptability within the organisation of internal audit?
- Has the risk profile of the entity changed so as to impact on the adequacy of internal audit?[145]

5. Risk management The audit committee will ensure that there is an effective system of risk management within the organization and that this system supports the controls which, in turn, provide a reasonable expectation of achieving organizational objectives. The audit committee will ensure that risk management is carried out in a consistent and professional manner and is integrated into the working practices and decision-making mechanisms throughout the organization. The committee will also ensure that the reporting of risk (in the form of risk registers) is coordinated and actioned in line with the corporate risk policy and strategies and that:

- there is a formal process for identifying, assessing and managing risk in all levels of the organization;
- a risk policy and strategy are in place and form the basis for dealing with risk;
- the risk policy is driven by a board member and the board ensures the process is efficient and effective;
- executives, senior management, team leaders and all staff understand their roles in respect of risk management and are discharging their responsibilities in a professional manner;
- training, awareness seminars and ongoing development are available and provided to employees wherever appropriate;
- the appropriate structures and arrangements are in place to ensure effective risk management;
- reports are provided to executives to enable them to monitor the implementation of the adopted risk management strategy;
- risk management is continually updated to reflect current positions and changes;
- risk registers are prepared that feed into the assurances to support the statement on internal control.

6. Compliance and propriety An oversight of systems and procedures is in place to ensure compliance with regulations, policies, laws and procedures and the organization's code of conduct. Also ensure that the organization is able to prevent, detect and respond to fraud and allegations of fraud. To this end, the AC should be able to:

- review systems in place to promote compliance including staff awareness events;
- review the code of conduct and receive summary reports on violations along with any resulting action against the employee in question;
- receive regular reports from the chief compliance officer (or ethics officer) on the reliability and development of standards of conduct;
- ensure the organization has in place suitable controls that act as safeguards against fraud and irregularity;
- ensure employees are aware of the risk of fraud and that this risk is always incorporated in the risk assessment/management process at all levels in the organization;
- ensure there is a clear facility to ensure all suspicions of fraud are reported to the appropriate person and that there are procedures designed to detect fraud and abuse if they occur;
- ensure there is a capacity to investigate all allegations of fraud and abuse and that these investigations are conducted in a professional manner in conjunction with laws and regulations concerning such investigations;
- ensure confidential progress and final reports are made for significant investigations that impact the reputation of the organization;

- ensure lessons are learnt for all problems where controls have failed or the response could have been better and these lessons have been incorporated into new procedures or staff development programmes;
- ensure emerging high-risk areas where legal provisions may be misunderstood are addressed by the organization – an example being partnership projects and e-business ventures.

More recently, there has been a move to establish risk committees to take charge of advising the board regarding the oversight of the risk management process as a specialist area of expertise.

7. Financial management To consider the finances and expenditure of the organization and ensure that:

- there is a good financial reporting system in place and that this feeds properly into the process for preparing the annual accounts;
- there is a suitable budgeting system in place based on defined delegated authorities and financial limits;
- the scope for financial misreporting is minimized and that there are tight controls over areas where professional judgement is open to different interpretations;
- concerns by the external audit regarding the financial statements are addressed and resolved so as to reduce the level of potentially misleading information presented in the final accounts;
- financial information should meet quality standards as defined by professional practice and the chief finance officer (CFO);
- whether aggressive income reporting practices are in place and whether this creates undue pressure to impair objectivity in making judgements on the way accounting policies are applied. In some organizations, the main task of an audit committee is to make sure all income and expenditure is accounted for. As one extract from a church AC report demonstrates:

> Based on our review of financial, budgeting, and other controls and our review of xyz audit reports for 1999 and responses thereto, the Audit Committee is of the opinion that, in all material respects, church contributions received and expenditure during the year ended 31 December 1999 have been managed in accordance with revelation and established policies and procedures

8. Special investigations The audit committee may request special investigation from the IA, compliance officer, external auditor and external specialists where there is a need to probe into sensitive problems that fall within its remit. Special investigations will tend to happen in unusual areas where there are sensitive issues relating to audit, accountability and conduct. In contrast, general enquiries by the AC may revolve around areas of high risk, which may be highlighted in reports from risk registers using the Green, Amber and Red format (see Chapter 3) – where the AC will want to know that Red risks are being addressed by the risk owner and monitored by the executive.

The Audit Committee's Constitution

The role of the audit committee's chair is important and this should not be undertaken by the chairperson of the board of directors. However, research suggests that the board's chairperson still has a great deal of influence, albeit informal, over the AC. The committee will need a formal constitution to enable it to discharge its role effectively. The Treadway Committee in the US felt

that ACs help deter fraud and they are mandatory for companies quoted on the NYSE. Treadway said that: 'The mere existence of an audit committee is not enough. The audit committee must be vigilant, informed, diligent and probing.' The constitution will depend on the organization in question, but may incorporate some of the following matters:

1. Principal role The AC has been adopted by the board on xyz to provide support to the board and help them discharge their duty to maintain an oversight of the quality, professionalism and integrity of the accounting, auditing, risk management internal control, compliance issues, employee conduct and financial reporting practices, and the overall corporate governance arrangements. The AC has to request investigations into any issues that impact on their main role and additional duties may be assigned to the AC by the board. The committee will furnish an annual report to the board on the performance of internal control, and the performance of IA, EA and control self-assessment exercises. While the audit committee gives stakeholders some comfort that their investment is under control, there is still an overriding bond between the board and the AC in most large organizations. This bond has been commented on:

> An audit committee's first responsibility is to protect all board members from developments that are either illegal or otherwise so damaging that they threaten the public standing and welfare of the organization . . . Finally and most importantly, the audit committee acts as a 'court of last resort' where internal audit can potentially communicate any concerns that go beyond the responsibilities of senior management in the organization.[146]

2. Membership Members are appointed by the board, and the AC should consist of at least three members (and not more than six) being independent non-executive directors. Members should abide by a formal code of conduct drafted with their special responsibilities in mind. Members should be sufficiently independent to ensure they are able to discharge their obligations and this should be reconsidered by the committee at least annually. Any matter that interferes with an audit committee member's independence should be disclosed at the earliest opportunity. Where this matter cannot be resolved, the audit committee members should stand down or refrain from attending (or voting at) the meeting that is affected by the matter in question. Members should continue until their term has expired and cannot be elected for more than two terms. The length of service should balance the need for fresh and objective mindsets and the need for some continuity. Independence in directors working for a company is a wonderful aspiration, but as Andrew Chambers has noted, can cause some problems: 'There is nothing like the notion of "independence" to rattle the timber of the non-executive director. To pin it down is like nailing jelly to the ceiling.'[147]

3. Competence The AC should be equipped to discharge its obligations resulting from its agreed charter. This includes training, development, access to relevant information and reports and advice from specialist and technical personnel where appropriate. The organization should define a set of competencies applicable to AC member and ensure the appointments procedure is designed around these competencies. At least one member of the AC should have extensive experience in financial accounting and financial management. And at least one other member should have experience in corporate legal affairs and compliance requirements. The other members should either have experience of serving on an audit committee or undergo an induction programme performed by external specialists. AC members should demonstrate a degree of professional scepticism in assessing the corporate governance arrangements in the

organization and be able to challenge unusual practices or areas where there is poor information. Members should have a good understanding of the organization's business and should visit locations and the occasional management meeting to maintain sufficient knowledge of operations and performance.

4. Meetings Meetings should be held at least four times a year and all members should attend unless there are exceptional circumstances. Excessive levels of absence (e.g. less than 80%) by committee members may lead to their disqualification. A quorum shall be either three members or 50% of the membership. No committee member should have so many seats on company boards or committees so that it interferes with their ability to attend audit committee meetings or reduces the amount of time available to prepare for meetings. All papers should be provided in advance to committee members and should include a summary top sheet that encapsulates key issues (cross-referenced to the main report/papers). Papers may only be tabled at audit committee meetings where the chair has agreed that any delays in attending to the papers would be against the interests of the organization. Meetings should be long enough to ensure all main agenda items are considered in sufficient detail.

5. Reporting lines The audit committee shall make recommendations to the main board and furnish a copy of its minutes to the board members. The audit committee will have unrestricted access to the external auditor, CAE, legal officer, CEO, CFO and other officials and employees where appropriate and be able to meet with these individuals in private. The committee will also have access to external consultants and specialists where it furthers the objectives as set out in the AC charter. Parties that are required to attend AC meetings (such as the internal and external auditor) should present their role and approach in any induction programme. Regular training events should be held for audit committee members whenever there is a significant development in corporate governance codes or guidelines or where global events demonstrate that committee members need to address new areas of interest.

6. Authorities The AC has access to all organization records, information, personnel and buildings where this is necessary to discharge its obligations under its agreed objectives. The AC is able to commission and set the terms of reference for special investigations and receive the resultant reports in confidence where the investigation falls in line with its objectives. The audit committee will have access to legal advice where it needs to make a decision that may cause a legal liability for its members.

7. Development The AC should set clear criteria for assessing its performance which are prepared by a specialist and confirmed by the main board. The committee should then perform an annual assessment of the extent to which it meets its performance criteria, and report the results to the main board. The AC may wish to perform a facilitated control and risk self-assessment exercise to prepare its own risk register and action plan as part of its documented risk management arrangements. Meanwhile, the committee should be given a formal presentation on the current trends in the organization's business environment, corporate strategy, and key changes and project at least once every two years. The AC will need to demonstrate that it adds value to the organization's corporate governance arrangements set against the costs of maintaining such a committee.

It is probably a good idea for the AC to commission a handbook to cover the audit committee's roles and constitution and signposts to important aspects of the business that committee members need to understand. There should also be brief sections on all the matters included above. The

AC handbook could then be used to benchmark the performance of the committee and competence of its members. Note that many corporate governance codes call for a separate nominations committee, which is responsible for considering the size and composition of the board, criteria for board membership and proposing candidates for board membership; and a remunerations committee, which covers directors' fees and bonuses. Some organizations have set up a specialist Corporate Governance Committee, which reviews the board and the overall corporate governance arrangements.

The Internal Audit Perspective

The developing significance of the AC has gone hand in hand with more reliance on internal auditing as a key aspect of the corporate governance solution. In 2002, the NYSE Rules made it clear that 'each listed company must have an internal audit function'. In the UK, IA while strongly encouraged, is not mandatory (although audit committees are required). The internal auditor needs to have regard to their audit committee and appreciate that this group forms a key customer. This simple concept is forcefully presented by an article in *Internal Auditor*:

> The audit committee is a primary customer of the internal audit function. When the needs of a key customer change, the internal audit function must change accordingly or risk losing its traditional role. As more is demanded of audit committees, internal audit professionals should seize the opportunity to augment their services. Extending and expanding the interaction between audit committees and internal auditors can enhance the quality of corporate governance and strengthen the organizational infrastructure.[148]

One key area in which IA has a dominating expertise is in applying control models to an organization, and it is here that the CAE may help the AC understand the use and design of control models through which to base any view of internal controls that they might recommend to the main board. Many IA shops have a dotted line responsibility to the AC. While bearing this in mind, the internal auditor should also ensure there is a clear relationship between the CAE and the executive board, with reference to IIA Performance Standard 2060 on Reporting to the senior management and the board:

> The chief audit executive must report periodically to senior management and the board on the internal audit activity's purpose, authority, responsibility, and performance relative to its plan. Reporting must also include significant risk exposures and control issues, including fraud risks, governance issues, and other matters needed or requested by senior management and the board.

Meanwhile, the IIA definition of internal auditing takes the CAE into the heart of the AC's role and provides a platform to launch assurance and consulting work on *risk management, control and governance processes*. This is pretty much the language of the NEDs as well as the executives on the board members. The AC will want to know about IA's work but the CAE must be very careful not to turn this committee into a venue for second guessing top management. The type of information given to the AC should be framed with this consideration in mind.

A further issue for the internal auditor is deciding what triggers a special report to the audit committee. Anthony J. Ridley has suggested that this can be considered in advance and criteria established with the committee so that a common understanding of what is needed ensures speed, clarity and efficiency in passing on relevant information. Each type of event is assigned a code A–D where:

A – notify AC immediately

B – at next AC meeting

C – annual report

D – annual summary.

The codes are assigned to events such as fraud, ethics violation, serious audit finding and so on along with details of impact measures (e.g. value or national press coverage). [149]

Some audit committees get intimately involved in the IA product and see copies of all reports issued by the CAE. One extract from an Audit Oversight Committee includes the following procedures: 'The final internal audit report will be filed with each member of the Audit Oversight Committee, copy to the external auditor if appropriate, copy to the CEO and each member of the Board of Supervisors.'

An even more worrying position is assumed by some audit committees where they actually become an explicit part of the IA process as another extract from an organization's procedures suggests:

> Following a study of a particular area selected for examination, the internal auditor draws up a draft report with appropriate recommendations. This is referred for comment to those who were subject of the study before consideration by the audit committee (AC), which determines, in the light of all comments, the extent to which the internal audit recommendations should be implemented. The AC decisions are then communicated to those in power to implement the recommendations and, at a later stage, the AC will seek a report on progress.

The AC must be able to address the real issues if it is to have any use at all. One further setback is where the AC members have little understanding of systems, controls, financial procedures, fraud, corporate governance and other issues relating to officer accountability. It is as well to provide regular presentations to the committee on each of these topics and so ensure that it is able to understand the audit issues and audit reports. The original King report provided a comprehensive consideration of a wide aspect of corporate governance arrangements and its guidance on the AC is designed to promote its independence as fundamental to its proper functioning. It includes the following key matters:

- The board should appoint an audit committee that has a majority of independent non executive directors. The majority of the members of the audit committee should be financially literate. (para. 6.3.1)
- The chairperson should be an independent non executive director and not the chairperson of the board. The better view is that the board chairperson should not be a member of the audit committee at all, but could be invited to attend meetings as necessary by the chairperson of that committee. The board should consider whether or not it is desirable for the chief executive to be a member of the audit committee, or to attend only by invitation. (para. 6.3.2)
- The audit committee should have written terms of reference that deal adequately with its membership, authority and duties. (para. 6.3.3)
- Companies should, in their annual report, disclose whether or not the audit committee has adopted formal terms of reference and, if so, whether the committee has satisfied its responsibilities for the year, in compliance with its terms of reference. (para. 6.3.4)
- Membership of the audit committee should be disclosed in the annual report. The chairperson of the committee should be available at the annual general meeting to answer questions about its work. (para. 6.3.5)

Public Sector (Government) Audit Committees

The public sector is designed around democratic elections where the public, after each term, may vote out a government if they fail to perform. Meanwhile, there are normally layer upon layer of accountability mechanisms imposed on public bodies like trusts, committees, inspectors, regulators, financial regulations, auditors, public enquiries, ombudsman and so on. For some years, there has been some resistance to the idea of audit committees from parts of the public sector, such as local government. The point has been missed that the AC has a specialist role to consider audit and accountability and more recently corporate governance in whatever organizations it is established. Even where there is a non-executive trust board, or oversight committee, or monitoring body, there is nonetheless a growing trend towards establishing formal audit committees in all parts of government and wider public bodies. The IIA have prepared a position statement called the Audit Committee in the Public Sector which suggests:

> The Institute recommends that a public sector entity establish an audit committee as a standing committee of the governing body . . . The tasks, responsibilities, and the goals of management, audit committee, and internal auditors are closely intertwined in many ways. As the demand for enhanced accountability and quality of services in the public sector increases, so does the significance of the internal auditor/audit committee relationship. The audit committee has a major responsibility in assuring that the mechanisms for achieving accountability and for reducing the risk of management override are in place and functioning. Clearly, one of these mechanisms is a solid, well-orchestrated, cooperative relationship with the internal auditors. This position statement is a step toward promoting that type of relationship by helping the audit committee and internal auditors work together. Together they can achieve the common goals of quality of services for the citizens and accountability over the use of public funds.

Meanwhile the HM Treasury have produced a document entitled 'Policy Principles for Audit Committees in Central Government', which includes the following advice that establishes this forum with the government sector:

> The purpose of an Audit Committee (AC) is to give to the Accounting Officer (AO) on the adequacy of audit arrangements (internal and external) and on the implications of assurances provided in respect of risk and control in the organisation.

1. ACs are strongly encouraged as best practice in all central government bodies . . .
2. The AC should be a sub-committee of the board . . .
3. In bodies that have NEDs these NEDs should form at least part of the membership of the AC.
4. Where there are no NEDs, appropriate external members should be sought to form at least part of the membership of the AC.
5. The AC should ideally have between five and ten members . . .
6. The AC is appointed to give advice to the AO. Although the AO may chair, the objectivity of the advice given can be enhanced if another member (particularly a NED) is the chair of the AC.
7. Members of the AC who have executive responsibility . . . should be rotated on a three year cycle . . .
8. AC should have a documented TOR which should include a remit to consider the adequacy of risk management and internal control through reviewing:
   - mechanisms for assessing and management of risk.

- planned activity of internal audit (IA).
- results of IA activity.
- planned activity of external audit (EA).
- results of EA activity.
- adequacy of management response to issues.
- identified by audit activity.
- assurances relating to the corporate governance requirements for the organisation.

9. The CAE and the senior member of the EA team should have the right of access to the AC and should normally be present at meetings (as attendees rather than members).
10. The AC should meet regularly and at least three times a year.[150]

The NYSE Rules

The American business scandals that broke in 2002 led to a revision in the listing rules set by the NYSE.

(i) (a) Increase the authority and responsibilities of the audit committee, including granting it the sole authority to hire and fire independent auditors, and to approve any significant non-audit relationship with the independent auditors.

(b) The audit committee must have a written charter that addresses:

(i) the committee's purpose – which, at minimum, must be to:

(A) assist board oversight of (1) the integrity of the company's financial statements, (2) the company's compliance with legal and regulatory requirements, (3) the independent auditor's qualifications and independence, and (4) the performance of the company's internal audit function and independent auditors; and

(B) prepare the report that SEC rules require be included in the company's annual proxy statement.

(ii) the duties and responsibilities of the audit committee – which, at minimum, must be to:

(A) retain and terminate the company's independent auditors (subject, if applicable, to shareholder ratification).

(B) at least annually, obtain and review a report by the independent auditor describing: the firms' internal quality-control procedures; any material issues raised by the most recent internal quality-control review, or peer review, of the firm, or by any inquiry or investigation by governmental or professional authorities, within the preceding five years, respecting one or more independent audits carried out by the firm, and any steps taken to deal with any such issues; and (to assess the auditor's independence) all relationships between the independent auditor and the company.

(C) discuss the annual audited financial statements and quarterly financial statements with management and the independent auditor, including the company's disclosure under 'Management's Discussion and Analysis of Financial Condition and Results of Operations.'

(D) discuss earnings press releases, as well as financial information and earnings guidance provided to analysts and rating agencies.

(E) as appropriate, obtain advice and assistance from outside legal, accounting or other advisors.

I. discuss policies with respect to risk assessment and risk management.

II. meet separately, periodically with management, with internal auditors (or other personnel responsible for the internal audit function) and with independent auditors.
III. review with independent auditor any audit problems or difficulties and management's response.
IV. set clear hiring policies for employees or former employees of the independent auditors.
V. report regularly to the board of directors.

(iii) an annual performance evaluation of the audit committee.

Developing the Audit Committee

Professor Jeff Ridley has suggested the use of self-assessment of the audit committee as a way of measuring performance and has developed six steps to a successful audit committee:

1. Independence.
2. Rotation of members.
3. Unrestricted responsibility.
4. Monitoring of all control.
5. Provides advice only.
6. Reports results of its work to the board and externally.

He also argues that 'the AC should compile an annual report to shareholders within the annual report or as a separate statement'.[151]

This final point has now been adopted by the NYSE, and sticking to guides to best practice, Larry Rittenberg has developed several lessons for internal auditors as follows:

Lesson 1 – Corporate Governance is important.

Lesson 2 – Reporting structure does matter – CAE access to AC.

Lesson 3 – Accounting issues and controls are important – financial reporting.

Lesson 4 – Risk is the dominant framework for internal audit – including financial risk.

Lesson 5 – The audit committee needs an effective information system – based on Blue Ribbon Committee rules.

Lesson 6 – Auditors must understand the business – particularly external auditors.

Lesson 7 – Auditors can assist in educating board and audit committee members – eg self evaluation by the AC.

Lesson 8 – Related party transactions and complex financial instruments present substantial risks.

Lesson 9 – Reporting is a process, not an event – audit reports.

Lesson 10 – Commit to continuous improvement – IA as leaders in technology, security and control.[152]

DTI Review of Audit and Accountability

The pivotal role of the AC as a representative of shareholders and independent bridge between the external auditors, the board and management has been recognized in the 2002 DTI review.

The resulting DTI recommendations have thrust the audit committee into the heart of corporate governance, as is clear from extracts from their recommendations for the new look role of the audit committee:

- Monitor the integrity of the company's financial controls and financial policies;
- Be responsible, and be seen publicly to be responsible, for recommending to shareholders the appointment and/or re-appointment of the external auditors;
- Be responsible, and be seen publicly to be responsible, for approving the provision of non-audit services by the auditor;
- Be an independent element in the relationship between the company management and the auditor;
- Review the quality of the audit process and audit judgment, including a review of auditor independence; and
- Report annually to shareholders on how it has discharged its responsibilities. (para. 4.4)

> The Combined Code already contains a provision that where auditors also supply a substantial volume of non-audit services to the company, the Audit Committee should 'keep the nature and extent of such services under review, seeking to balance the maintenance of objectivity and value for money'. (para. 4.5)
>
> We strongly support the view that an effective Audit Committee, with clear responsibilities, and reporting to shareholders, can play a key role on behalf of the shareholders in driving up audit quality and preserving auditor independence. More can be done to develop the role of Audit Committees. (para. 4.9)

The IIA has posted material on its website on Internal Auditing and the Audit Committee: Working Together Toward Common Goals, which concluded that:

> The tasks, responsibilities, and goals of audit committees and internal auditing are closely intertwined in many ways. Certainly, as the magnitude of the 'corporate accountability' issue increases, so does the significance of the internal auditing/audit committee relationship. The audit committee has a major responsibility in assuring that the mechanisms for corporate accountability are in place functioning. Clearly, one of these mechanisms is a solid, well-orchestrated, co-operative relationship with internal auditing. The Institute of Internal Auditor's Position on Audit Committees is a step toward promoting that type of relationship – helping audit committees and internal auditing work together toward common goals.[153]

The Smith Report

The draft report by Sir Robert Smith was submitted to the Financial Reporting Council and contained various recommendations for changes to the code of practice for listed companies as follows:

D.3 Audit Committee and Auditors

Principle The board should establish formal and transparent arrangements for considering how they should apply the financial reporting and internal control principles and for maintaining an appropriate relationship with the company's auditors.

Code provisions

D.3.1 The board should establish an audit committee of at least three members, who should all be independent non-executive directors. At least one member of the audit committee should have significant, recent and relevant financial experience.

D.3.2 The main role and responsibilities should be set out in written terms of reference and should include:

(a) to monitor the integrity of the financial statements of the company, reviewing significant financial reporting issues and judgements contained in them;
(b) to review the company's internal financial control system and, unless expressly addressed by a separate risk committee or by the board itself, risk management systems;
(c) to monitor and review the effectiveness of the company's internal audit function;
(d) to make recommendations to the board in relation to the appointment of the external auditor and to approve the remuneration and terms of engagement of the external auditor;
(e) to monitor and review the external auditor's independence, objectivity and effectiveness, taking into consideration relevant UK professional and regulatory requirements;
(f) to develop and implement policy on the engagement of the external auditor to supply non-audit services, taking into account relevant ethical guidance regarding the provision of non-audit services by the external audit firm.

D.3.3 The audit committee should be provided with sufficient resources to undertake its duties.

D.3.4 The directors' report should contain a separate section that describes the role and responsibilities of the committee and the actions taken by the committee to discharge those responsibilities.

D.3.5 The chairman of the audit committee should be present at the AGM to answer questions, through the chairman of the board.

2.8 Internal Audit

The *Internal Auditing Handbook* is primarily about the role, responsibilities and performance of the IA function. This section simply provides a brief account of where IA fits into the corporate governance jigsaw. The IIA have prepared performance standard 2110 on this issue which says: 'The internal audit activity must assess and make appropriate recommendations for improving the governance process in its accomplishment of the following objectives:

- promoting appropriate ethics and values within the organization;
- ensuring effective organizational performance management and accountability;
- communicating risk and control information to appropriate areas of the organization; and
- coordinating the activities of and communicating information among the board, external and internal auditors, and management'

This enables us to place IA into our corporate governance model in Figure 2.9.

There is much guidance to turn to for help in reinforcing the IA position. Gill Bolton has provided advice for auditors about implementing the Turnbull provisions on corporate governance:



FIGURE 2.9 Corporate governance (6).

Working with the board, the AC and the risk committee (where it exists) to embed risk management and internal control into the organization as a whole, IA is likely to be the only function within an organization that has deep understanding of risk and control:

- Providing risk management and control advice to relevant staff across the organization.
- Providing independent and objective assurance to the board about the adequacy and effectiveness of key controls and other risk management activities across the organization.
- Acting as risk and control educators across the organization.[154]

While most parts of the public sector have adopted codes that require the existence of internal audit, some parts have enshrined the role of internal audit in legislation, and not only best practice guides. Under the Local Government Act 1972, section 151, every local authority shall make arrangements for the proper administration of their financial affairs and shall secure that one of the officers has responsibility for the administration of those affairs. This meant that the officer, e.g. finance officer, had to maintain an internal audit function. The Accounts and Audit Regulations of 1983 required the responsible financial officer to maintain an adequate and effective internal audit of the accounts of the body. Of late, the 1996 regulations meant that the head of finance need not now have direct control over the internal auditing function of the council, while larger organizations – universities, housing associations, health trusts, or other not-for-profit bodies – all have codes that require internal audit and it is becoming hard to find any organization of size that does not have internal audit.[155]

Basle Committee on Banking Supervision

The specialist code applicable to the international banking sector contains many important provisions that contribute to the internal auditing provisions for good corporate governance. A summary version based on the draft July 2000 report follows (www.bis.org):

Principle 1 – Board ultimately responsible for RM and IC.

Principle 2 – Senior management identify, measure and monitor control risk.

Principle 3 – The IA function is part of the ongoing monitoring of the system of internal controls and of the bank's capital assessment procedure, because it provides an independent assessment

of the adequacy of, and compliance with, the bank's established policies and procedures. As such, the internal audit function assists members of the organisation in the effective discharge of their responsibilities . . .

Principle 4 – Internal audit in the bank should be a permanent function . . .

Principle 5 – The bank's internal audit department must be independent of the activities audited . . .

Principle 6 – An audit charter guarantees the standing and authority of the internal audit department within the bank . . .

Principle 7 – The internal audit department (IAD) should be objective and impartial, which means it should be in a position to perform its assignments free from bias and interference.

Principle 8 – The professional competence of every internal auditor and of the IAD as a whole is essential for the proper functioning of the bank's internal audit function.

Principle 9 – Every activity and every entity of the bank should fall within the scope of the IA.

Principle 10 – Within the framework of the bank's internal capital assessment process, the bank's IAD should carry out regularly an independent review of the measurement system for assessing the various risks faced by the bank, the system developed by the bank to relate risk to the bank's capital level, and the method established for the monitoring compliance with internal capital policies.

Principle 11 – IA includes drawing up an audit plan, examining and assessing the available information, communicating the results, and following up recommendations and issues.

Principle 12 – The head of the IAD should be responsible for ensuring that the department complies with sound IA principles.

Principle 13 – The board of directors should ensure that senior management establishes an internal control system and a capital assessment procedure and reviews them once a year. At least once a year, senior management should report to the board of directors on the scope and performance of the internal control system and of the capital assessment procedure. Bank supervision can evaluate the work of the IAD and, if satisfied, can rely on it to identify areas of potential risk.

Principle 14 – Supervisory authorities should have periodic consultations with the bank's internal auditors to discuss the risk areas identified and measures taken. At the same time, the extent of the collaboration between the bank's IAD and the bank's external auditors may also be discussed.

Principle 15 – Supervisors are encouraged to arrange regular discussions of policy issues jointly with the chief internal auditors of the banks under their supervision.

Principle 16 – Supervisory authorities should encourage consultation between internal and external auditors in order to make their cooperation as efficient and effective as possible.

Principle 17 – Work performed for a bank's supervisory authority by an external auditor should have a legal or contractual basis. Any task assigned by the supervisory authority to the external auditor should be complementary to his/her regular audit work and should be within his/her competence.

Principle 18 – Cooperation among the supervisor, the external auditor and the internal auditor aims to make the contribution of all concerned parties more efficient and effective in order to

optimise supervision. The cooperation may be based on periodic meetings of the supervision and the external and internal auditor.

Turnbull on Internal Audit

This report provides more support for the IA function and paragraphs 42 to 47 contain the following provision on IA:

- Provision D.2.2 of the Code states that companies which do not have an internal audit function should from time to time review the need for one. (para. 42)
- The need for an internal audit function will vary depending on company-specific factors including the scale, diversity and complexity of the company's activities and the number of employees, as well as cost/benefit considerations. Senior management and the board may desire objective assurance and advice on risk and control. An adequately resourced internal audit function (or its equivalent where, for example, a third party is contracted to perform some or all of the work concerned) may provide such assurance and advice. There may be other functions within the company that also provide assurance and advice covering specialist areas such as health and safety, regulatory and legal compliance and environmental issues. (para. 43)
- In the absence of an internal audit function, management needs to apply other monitoring processes in order to assure itself and the board that the system of internal control is functioning as intended. In these circumstances, the board will need to assess whether such processes provide sufficient and objective assurance. (para. 44)
- When undertaking its assessment of the need for an internal audit function, the board should also consider whether there are any trends or current factors relevant to the company's activities, markets or other aspects of its external environment, that have increased, or are expected to increase, the risks faced by the company. Such an increase in risk may also arise from internal factors such as organisational restructuring or from changes in reporting processes or underlying information systems. Other matters to be taken into account may include adverse trends evident from the monitoring of internal control systems or an increased incidence of unexpected occurrences. (para. 45)
- The board of a company that does not have an internal audit function should assess the need for such a function annually having regard to the factors referred to in paragraphs 43 and 45 above. Where there is an internal audit function, the board should annually review its scope of work, authority and resources, again having regard to those factors. (Para. 46)
- If the company does not have an internal audit function and the board has not reviewed the need for one, the Listing Rules require the board to disclose these facts. (Para. 47)

King Report

The original King report from South Africa also gave IA a key role in corporate governance arrangements:

4.1 Internal Audit

4.1.1 Companies should have an effective internal audit function that has the respect and cooperation of both the board and management. Where the board, in its discretion, decides not to establish an internal audit function, full reasons must be disclosed in the company's annual report, with an explanation as to how assurance of effective internal controls, processes and systems will be obtained.

4.1.2 Consistent with the Institute of Internal Auditors' ('IIA') definition of internal auditing in an internal audit charter approved by the board, the purpose, authority and responsibility of the internal audit activity should be formally defined.

4.1.3 The IIA has succinctly set out the role and function of internal audit in its standards for the professional practice of internal auditing, including the code of ethics and definition of internal audit which is fully endorsed by the King Committee.

4.1.4 Internal audit should report at a level within the company that allows it to fully accomplish its responsibilities. The head of internal audit should report administratively to the chief executive officer, and should have ready access to the chairperson of the company and the chairperson of the audit committee.

4.1.5 Internal audit should report at all audit committee meetings.

4.1.6 The appointment or dismissal of the head of the internal audit should be with the concurrence of the audit committee.

4.1.7 If the external and internal audit functions are carried out by the same accounting firm, the audit committee and the board should satisfy themselves that there is adequate segregation between the two functions in order to ensure that their independence is not impaired.

4.2 Scope of Internal Audit

4.2.1 Internal audit is an independent, objective assurance and consulting activity to add value and improve a company's operations. It helps a company accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.

4.2.2 An effective internal audit function should provide:

assurance that the management processes are adequate to identify and monitor significant risks;

confirmation of the effective operation of the established internal control systems; credible processes for the effective feedback on risk management and assurance; and objective confirmation that the board receives the right quality of assurance and information from management and that this information is reliable.

4.2.3 The internal audit plan should be based on risk assessment as well as on the issues highlighted by the audit committee and senior management. The risk assessment process should be of a continuous nature as to identify not only residual or existing but emerging risks and should be conducted formally at least annually, but more often in complex organisations.

4.2.4 The audit committee should approve the internal audit plan.

4.2.5 The internal audit function should co-ordinate with other internal and external providers of assurance to ensure proper coverage of financial, operational and compliance controls and to minimise duplication of effort.

We have referred to just a few of the codes and provisions for IA in the wake of moves to further the development of stronger corporate governance. The door has been opened for the once low profile audit teams that they may enter through and access the boardroom agenda. Moreover, the internal auditor can be the best friend of the AC and perhaps one of the few parties that can be relied on to give impartial and reliable advice and information. This growing expectation represents a major opportunity to staff up the audit team with people who can provide sound strategic level judgements to senior officials in a move away from the desk-based and detailed analysis typically provided to junior management.

2.9 The Link to Risk Management and Internal Control

We have said that the role of internal auditing incorporates coverage of risk management, control and governance processes. It is a good idea to briefly establish the links between these three ideas so that while each chapter deals with each of the three concepts, they can be appreciated both separately and together. Figure 2.10 may help explain the links.

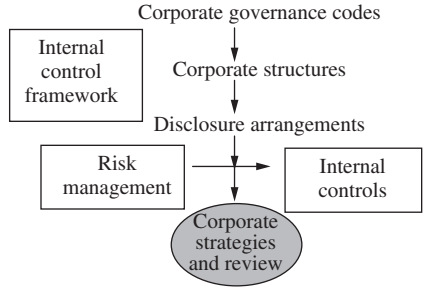


FIGURE 2.10 Linking RM to internal control.

Looking at each part of the model in turn:

Corporate governance codes: These are essentially the codes, guides, regulations and standards that, apart from family-run concerns, cover most larger organizations.

Corporate structures: The governance structures and processes include all those arrangements to ensure compliance with the governance codes. This includes, boardroom arrangements, splitting the CEO's and chair's roles, codes of conduct, audit committees, NEDs, internal and external audit and so on.

Disclosure arrangements: The matters that have to be included in the annual report including the audited accounts, external audit report, notes to the accounts, directors' report and operational review. This also includes disclosures on compliance with corporate governance codes, risk management arrangements and a statement on internal control.

Internal control framework: We deal with internal control in Chapter 4. For our model, we argue that all large organizations should adopt a control framework that sets out its vision of control. This provides a road map regarding the control environment, how people relate to each other and communicate, corporate structures and governance processes mentioned above.

Risk management: Within the context of the control framework, the organization should employ a process for identifying, assessing and managing risk. Note that risk management is covered in Chapter 3.

Internal controls: After having assessed key risk, they will need to be managed in line with a defined risk management strategy. One major component of this strategy is appropriately derived

internal controls that seek to mitigate unacceptable levels of risk. Each control will address a defined risk or be part of a regulatory requirement that in turn addresses the risk of breaching law, procedures and rule.

Corporate strategies and review: The strategy for managing risk and ensuring controls do the job in hand should then be incorporated into an overall strategy that drives the organization towards the achievement of its objectives. The entire process should be directed, assessed, reviewed and improved in conjunction with a formal performance measurement system.

By considering the above components, we can see how corporate governance is the umbrella concept that drives a control and reporting framework, which in turn depends on risk management and an efficient system of internal control. The three big parts – governance, risk management and control – form an entire system that provides for effective performance and stakeholder accountability.

2.10 Reporting on Internal Controls

Sir Adrian Cadbury has said that corporate governance is about the way an organization is directed and controlled. If the board is in control of their business and they are adhering to all appropriate standards then stakeholders can take comfort in this fact. Meanwhile, being in control means that all foreseeable risks to the success of the business have been anticipated and addressed, as efficiently as possible. This alone does not guarantee success, but it does mean that there is a reasonable chance that the organization will maintain, if not exceed, market expectations. To underline the need to be in control, the published annual report for companies listed on the stock exchange and most public sector or bodies should include a statement of internal control. This statement is a bottom line item, which is derived from the complicated arrangement of systems, processes and relationships established within the organization. If these controls drive the organization forward and also tackle all known risks that threaten this positive direction, then there is a good system of internal control in place. A well-governed organization must have good controls and the statement of internal control represents a crucial vote of confidence from the board to the shareholders and other stakeholders. The Turnbull report includes a set of questions that the board may wish to discuss with management when considering reporting on internal control and carrying out its annual assessment. The list is based around the COSO model of control (see Chapter 4) and covers the following areas:

1. Risk assessment
2. Control environment and control activities
3. Information and communication
4. Monitoring

A brief consideration of a selection of published statements illustrates this theory:

> The Group Audit Committee has received and considered reports on the effectiveness of the groups' system of internal financial controls. These include an annual assessment of the state of controls from the internal audit function, reports from the external audits on matters identified during the course of their statutory audit work, a review of the work of each of the business audit committees, and management assurance of the maintenance of control. The latter is based on an annual letter or assurance by which responsible managers confirm the adequacy of their

systems of internal financial control, and their compliance with Group policies, local laws and regulations and report any control weaknesses identified during the past year.[156]

System of internal control – the system of internal control is based on a framework of regular management information and administrative procedures. The key elements of the system of internal financial control are:

- the preparation of the three year strategic plan
- regional and departmental plan
- performance indicators which measure financial and other targets
- established financial policies
- decision making procedures
- comprehensive budgeting system
- actual results compared to approved budgets

however such a system is designed to manage rather than eliminate risk of failure to achieve business objectives and can provide reasonable not absolute assurance against material misstatement or loss.[157]

It is clear from the above that the board can secure information on the functioning of internal controls from sources within the organization, with much of this coming from the risk management and assurance reporting process that has been established. The internal and external auditors also provide a major input as does the AC. Some organizations require their top managers to provide assurance statements where they confirm that suitable controls are in place, that they have been reviewed and improved (where appropriate) and that they are designed to help manage all material risks to the achievement of objectives. Moreover, the statements may also incorporate a consideration of whether the controls are being applied as intended and that they are reliable. IA is a big player in this field on control reporting and most audit teams have sharpened their focus to feed into the board's attestations (or chief executive for public sector organizations). However, this is not always straightforward as a flash survey of 414 responses by IIA's Global Auditing Information Network in April 2002 reveals. Extracts from their report follow:

Question 01: Does IA provide senior management or the audit committee with a written report on internal control? – 29.1% said No.

One comment – We do not provide a single report on internal control. However, internal controls are the primary focus on each review we do. Each audit of a particular function or area would generally include a review of the internal controls in that area, so any issues would be reported in that individual audit report.

Another comment – In reality what we give the audit committee and senior management is a copy of the Executive Summary Report for each internal audit, a letter that outlines significant control issues observed by external audit (management letter), and I present other issues at each audit committee meeting.

Other comment – An enterprise wide risk management system was initiated during 2001 and continues to grow. Control Self-Assessments are part of this process, and when complete, internal audit validates that the controls identified are adequate and consistently functioning as described.

Another comment – Reports to the audit committee are on an 'exception' basis, ie control breakdowns that have been identified during internal audits.

Another comment – Just summary reports based on audit projects. This is management's responsibility.

Another comment – Has not in the past, but will be reporting for the first time on the organisation's control environment by the end of the calendar year based on departmental internal control assessments.[158]

Internal Audit's Seat At The Governance Table

By Dan Swanson, *Compliance Week Columnist*

In June 1999, the Institute of Internal Auditors approved a new definition for internal auditing. Internal auditing was described as ''an independent, objective assurance and consulting activity,'' which isn't exactly news. Instead, the telling phrase came at the end of the revised IIA definition – which said internal auditing should be brought to bear on a company's risk management, internal control, and governance processes. For many years, the IIA has advocated that internal audit should be one of the cornerstones of good governance. The IIA has recently issued a global position statement regarding organizational governance that discusses the many roles that internal auditing can play in an organization's governance effort; a few are discussed in this month's column.

You Can Audit Governance?

Governance activities exist to help a company meet its objectives in being well run and accountable to its stakeholders. Just like in any other activity, management and the board will want to articulate their objectives in each area and put programs in place to achieve those objectives. An often-used definition of organizational governance comes from the Paris-based forum of democratic markets, the Organization for Economic Co-operation and Development (OECD): ''Corporate governance involves a set of relationships between a company's management, its board, its shareholders, and other stakeholders. Corporate governance also provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined.''

Components of governance that internal audit can provide assurance or consulting services include:

- Board structure, objectives, and dynamics
- Board committee functions
- The board policy manual
- Processes for maintaining awareness of governance requirements
- Board education and training
- Proper assignment of accountabilities and performance management
- Completeness of ethics policies and codes of conduct
- Communication and acceptance of ethics policies and codes of conduct
- Management evaluation and compensation
- Recruitment processes for senior management and board members
- Employee training
- Governance self-assessments
- Comparison with governance codes or best practices
- External communications

What Internal Audit Brings To The Table

Typically, internal auditors operate in two capacities regarding governance. First, auditors provide independent, objective assessments on the appropriateness of the company's governance structure and the operating effectiveness of specific governance activities. Second, they act as catalysts for change, advising or advocating improvements to enhance the organization's governance structure and practices. By providing assurance on the risk management, control, and governance processes within an organization, internal auditing is one of the cornerstones of effective organizational governance. In auditing the risk management processes used by the organization, internal audit might recommend that a more formal enterprise-wide, risk-management program be considered by the board and management. In consulting with the CEO or CFO, internal audit could recommend that the terms of reference for key organizational oversight committees (management's and the board's) be updated – and most likely expanded – to tackle the many emerging governance requirements facing most organizations today.

How To Earn That Seat At The Table

Auditing the financial transactions that have been processed within accounting is straightforward: Review for proper authorization, assess supporting evidence for appropriateness of transactions, test for accuracy and completeness of financial reporting, and then communicate your findings to management. By comparison, auditing governance can be complex and somewhat subjective. For example, try evaluating whether a proper ''tone at the top'' exists in the organization, or that the board and management reinforce the code of conduct properly – and follow it themselves!

Defining the scope of governance processes is a first step. What are we looking at, and who is responsible for what? Obtaining a consensus on what the performance measures are can be another challenging planning activity. Remember, in auditing governance you want to ensure the areas selected for review are ones that have the largest potential for improvement, or are in highest need of confirmation that they are operating effectively. Obtaining the support of your audit committee chairman and your CEO is absolutely critical. Having the skills and experience required to perform the audit task is also a must. What role internal audit plays in governance is highly influenced by the maturity level of the organization's governance processes and structure and the role and qualification of internal auditors. When there is much to do in formalizing and strengthening governance efforts, internal audit will likely focus more on providing advice regarding best structure and good practices to consider. Where governance is very structured and operating relatively effectively, the audit would likely focus on identifying further improvement opportunities and assessing the performance of key controls and practices. Benchmarking the company's governance practices to similar organizations could be very beneficial. Assessing compliance with published and respected governance codes could offer another quick win for internal audit and the organization.

Bringing Transparency To Governance Ask for a report card from internal audit; identifying improvement opportunities is the first step in continuous improvement.

Consider inviting your chief audit executive to provide an opinion on the organization's governance practices; it certainly will provide a learning opportunity for all the stakeholders involved in your organization, and obtaining an independent and objective assessment of this key activity (governing the organization) might just be what's needed to take your governance practices to the next level of transparency.

2.11 New Developments

After the WorldCom, Enron and Parmalat fiascos, the new millennium saw a new high in corporate malfunction with an array of amazing corporate headliners which includes:

Society Generale. The French bank Société Générale uncovered "an exceptional fraud" by a trader that would cost it nearly €5 billion. The fraud had been committed by a Paris-based trader in charge of "plain vanilla" hedging on European index futures.

Madoff. A major ponzi-type fraud was perpetrated by Bernard L Madoff, where he swindled wealthy investors and banks of huge amounts.

Parmalat. Fraud by Parmalat, an Italian dairy giant could be as much as $16.8 billion (far more than WorldCom) and may have been the result of more than a decade of fraudulent accounting.

Stanford. Sir Allen Stanford, the Antigua based American billionaire, philanthropist and cricket promoter and enthusiast, has been accused of a massive, $8 billion fraud by the US Securities and Exchange Commission (SEC).

During 2008, three of the largest US investment banks either went bankrupt or were sold at knock down prices to other banks.

Lehman Brothers. Just before it went under, plunging investor confidence in Lehman shares meant huge stock losses, while the US government stood back and watched, with no bail out plans in mind. As the crisis deepened some Lehman executives suggested that they would forgo million dollar bonuses as an example to their employees, but this was dismissed as unnecessary. Footage of Lehman staff removing their files and personal effects from HQ were beamed across the world as the reality of the credit crunch in action.

Merrill Lynch. Towards the end of 2007, Merrill Lynch announced it would write-down $8.4 billion in losses because of the national subprime housing crisis and removed its CEO and looked for the Bank of America to step in and buy it out.

Morgan Stanley/Goldman Sachs. Meanwhile, investment banks Morgan Stanley and Goldman Sachs responded to the financial crisis by embracing more rigorous regulatory as they became commercial banks. CEOs resigned and frantic search ensured for merger partners and government bailouts to keep the banking sector from going under. Meanwhile, over $100 billion were withdrawn from USA money funds, which meant the credit crunch brought the banking sector to the verge of a collapse. During the last quarter of 2008, these central banks purchased US$2.5 trillion of government debt and troubled private assets from banks.

Fannie Mae/Freddie Mac. World famous government-sponsored enterprises (GSE) Fannie Mae and Freddie Mac found themselves with trillions of dollars in mortgage obligations that were not supported by a weakened capital base, before being placed into receivership.

Northern Rock. Over in the UK, people queued outside of Northern Rock to withdraw their savings as the knock on effect hit the rest of the world while highly leveraged financial sector companies across the world were being bailed out by their governments or had to merge with stronger companies, as credit dried up. Northern Rock used to be a building society before it demutualized so that it could be floated on the London Stock Exchange and proceeded to buy up smaller building societies. Towards the end of 2007, the bank sought support from the Bank of England, which caused customers to panic and formed long queues to withdraw their savings. After dipping their toes into the US subprime mortgage market and failing, and with no clear takeover bids in place, they were effectively nationalized. At the start of 2009, Northern Rock announced that they would be offering £14 billion worth of new mortgages, over the next two years, as a part of their new business plan.

The 2007/08 Credit Crunch brought home the contrast between rapid short-term spurts of new business and steady growth that would be sustained in the long term. This point is brought home by the ACCA who submitted comments to the Financial Reporting Council (FRC);

> In the current challenging economic conditions there is an even greater need on the part of shareholders and, indeed, society as a whole to be able to have confidence in corporate reporting. A reliable audit, carried out by a properly competent firm should be a key component contributing to this confidence. It is important that audit firms are, and are seen to be, well governed. We recognise, therefore, the importance of this project and we support its objectives. We support the Combined Code and the 'comply or explain' approach for listed companies. However, as we have suggested in the past to the FRC, we consider the application of the Combined Code's principles to be at least as important as its provisions and so prefer what we refer to as an 'apply, comply or explain' approach. The current crisis affecting the banking sector has raised difficult questions about how well some organisations have applied the Combined Code's principles. In particular, there have been concerns about how shareholders engage with boards and boards engage with management. It would seem that such engagement to date has not been entirely in the long-tem interest of companies or their shareholders and other stakeholders and may even have encouraged the short-termist behaviour which has jeopardised the financial system.[159]

There is an ongoing debate about the way companies disclose information to their stakeholders. Reporting on specific disclosure issues does not always provide a rounded picture of how well the business is coping with material risks. Publicly traded companies in the UK now need to adhere with many different regulations that affect their corporate reports including:

- The Companies Act.
- International Financial Reporting Standards (IFRS) (for consolidated accounts).
- UK Generally Accepted Accounting Policies (GAAP) (for non-consolidated accounts).
- The Disclosure and Transparency Rules.
- The Listing Rules.
- The Combined Code on Corporate Governance.

The Financial Reporting Council has raised these concerns;

> Regulations are written with the best of intentions – but there is sometimes a difference between intended and actual outcomes. For example, a number of interviewees, both users and preparers, expressed concern that disclosures made in accordance with the minimum requirements of IFRS 7 Financial Instruments: Disclosures are not as useful as they might be. Part of the issue here is that the minimum disclosure requirements focus on specific instruments rather than the bigger picture, so meeting these requirements does not provide a good understanding of the risk management strategies used by management. This is interesting, because the standard is actually underpinned by the principle that information should be provided 'through the eyes of management'. Including a list of minimum disclosures in the standard has encouraged companies to comply with this list rather than providing information through the eyes of management; the result, according to many interviewees, is less useful information.[160]

Most agree that the task of achieving good governance in larger companies is an ongoing challenge. The UK's Combined Code tends to be reviewed by the FRC every two years or so and the 2009 review, taking on board the ramifications of the credit crunch, assessed the impact and effectiveness of the Code. Meanwhile the review by Sir David Walker was asked by the Prime Minister to review corporate governance, risk management and remuneration incentives in UK banks (then extended to other financial institutions) while the FRC will want to consider the extent to which the resulting recommendations may be considered best practice for all listed companies. The FRC have made it clear that they now wish to increase the overall level of prescription in the Code and to preserve its principles-based style.

The Walker review called for the risk management process to be given a much higher profile with greater independence in the group risk management function and the chief risk officer having a clear enterprise-wide authority and independence, with tenure and remuneration determined by the board. The final recommendations from the Walker Revew published in November 2009 are as follows:

Board size, composition and qualification

Recommendation 1 To ensure that NEDs have the knowledge and understanding of the business to enable them to contribute effectively, a BOFI board should provide thematic business awareness sessions on a regular basis and each NED should be provided with a substantive personalised approach to induction, training and development to be reviewed annually with the chairman. Appropriate provision should be made similarly for executive board members in business areas other than those for which they have direct responsibility.

Recommendation 2 A BOFI board should provide for dedicated support for NEDs on any matter relevant to the business on which they require advice separately from or additional to that available in the normal board process.

Recommendation 3 The overall time commitment of NEDs as a group on a FTSE 100-listed bank or life assurance company board should be greater than has been normal in the past. How this is achieved in particular board situations will depend on the composition of the NED group on the board. For several NEDs, a minimum expected time commitment of 30 to 36 days in a major bank board should be clearly indicated in letters of appointment and will in some cases limit the capacity of an individual NED to retain or assume board responsibilities elsewhere. For

any prospective director where so substantial a time commitment is not envisaged or practicable, the letter of appointment should specify the time commitment agreed between the individual and the board. The terms of letters of appointment should be available to shareholders on request.

Recommendation 4 The FSA's ongoing supervisory process should give closer attention to the overall balance of the board in relation to the risk strategy of the business, taking into account the experience, behavioural and other qualities of individual directors and their access to fully adequate induction and development programmes. Such programmes should be designed to assure a sufficient continuing level of financial industry awareness so that NEDs are equipped to engage proactively in BOFI board deliberation, above all on risk strategy.

Recommendation 5 The FSA's interview process for NEDs proposed for FTSE 100-listed bank and life assurance company boards should involve questioning and assessment by one or more (retired or otherwise non-conflicted) senior advisers with relevant industry experience at or close to board level of a similarly large and complex entity who might be engaged by the FSA for the purpose, possibly on a part-time panel basis.

Functioning of the board and evaluation of performance

Recommendation 6 As part of their role as members of the unitary board of a BOFI, NEDs should be ready, able and encouraged to challenge and test proposals on strategy put forward by the executive. They should satisfy themselves that board discussion and decision-taking on risk matters is based on accurate and appropriately comprehensive information and draws, as far as they believe it to be relevant or necessary, on external analysis and input.

Recommendation 7 The chairman of a major bank should be expected to commit a substantial proportion of his or her time, probably around two-thirds, to the business of the entity, with clear understanding from the outset that, in the event of need, the bank chairmanship role would have priority over any other business time commitment. Depending on the balance and nature of their business, the required time commitment should be proportionately less for the chairman of a less complex or smaller bank, insurance or fund management entity.

Recommendation 8 The chairman of a BOFI board should bring a combination of relevant financial industry experience and a track record of successful leadership capability in a significant board position. Where this desirable combination is only incompletely achievable at the selection phase, and provided that there is an adequate balance of relevant financial industry experience among other board members, the board should give particular weight to convincing leadership experience since financial industry experience without established leadership skills in a chairman is unlikely to suffice. An appropriately intensive induction and continuing business awareness programme should be provided for the chairman to ensure that he or she is kept well informed and abreast of significant new developments in the business.

Recommendation 9 The chairman is responsible for leadership of the board, ensuring its effectiveness in all aspects of its role and setting its agenda so that fully adequate time is available for substantive discussion on strategic issues. The chairman should facilitate, encourage and expect the informed and critical contribution of the directors in particular in discussion and decision-taking on matters of risk and strategy and should promote effective communication between executive

and non-executive directors. The chairman is responsible for ensuring that the directors receive all information that is relevant to discharge of their obligations in accurate, timely and clear form.

Recommendation 10 The chairman of a BOFI board should be proposed for election on an annual basis. The board should keep under review the possibility of transitioning to annual election of all board members.

Recommendation 11 The role of the senior independent director (SID) should be to provide a sounding board for the chairman, for the evaluation of the chairman and to serve as a trusted intermediary for the NEDs, when necessary. The SID should be accessible to shareholders in the event that communication with the chairman becomes difficult or inappropriate.

Recommendation 12 The board should undertake a formal and rigorous evaluation of its performance, and that of committees of the board, with external facilitation of the process every second or third year. The evaluation statement should either be included as a dedicated section of the chairman's statement or as a separate section of the annual report, signed by the chairman. Where an external facilitator is used, this should be indicated in the statement, together with their name and a clear indication of any other business relationships with the company and that the board is satisfied that any potential conflict given such other business relationship has been appropriately managed.

Recommendation 13 The evaluation statement on board performance and governance should confirm that a rigorous evaluation process has been undertaken and describe the process for identifying the skills and experience required to address and challenge adequately key risks and decisions that confront, or may confront, the board. The statement should provide such meaningful, high-level information as the board considers necessary to assist shareholders' understanding of the main features of the process, including an indication of the extent to which issues raised in the course of the evaluation have been addressed. It should also provide an indication of the nature and extent of communication with major shareholders and confirmation that the board were fully apprised of views indicated by shareholders in the course of such dialogue.

The role of institutional shareholders: communication and engagement

Recommendation 14 Boards should ensure that they are made aware of any material cumulative changes in the share register as soon as possible, understand as far as possible the reasons for such changes and satisfy themselves that they have taken steps, if any are required, to respond. Where material cumulative changes take place over a short period, the FSA should be promptly informed.

Recommendation 15 Deleted.

Recommendation 16 The remit of the FRC should be explicitly extended to cover the development and encouragement of adherence to principles of best practice in stewardship by institutional investors and fund managers. This new role should be clarified by separating the content of the present Combined Code, which might be described as the Corporate Governance Code, from what might most appropriately be described as the Stewardship Code.

Recommendation 17 The Code on the Responsibilities of Institutional Investors, prepared by the Institutional Shareholders' Committee, should be ratified by the FRC and become the Stewardship Code. By virtue of the independence and authority of the FRC, this transition to sponsorship by the FRC should give materially greater weight to the Stewardship Code. Its status should be akin to that of the Combined Code as a statement of best practice, with observance on a similar "comply or explain" basis.

Recommendation 18 The FRC should oversee a review of the Stewardship Code on a regular basis, in close consultation with institutional shareholders, fund managers and other interested parties, to ensure its continuing fitness for purpose in the light of experience and make proposals for any appropriate adaptation.

Recommendation 18B All fund managers that indicate commitment to engagement should participate in a survey to monitor adherence to the Stewardship Code. Arrangements should be put in place under the guidance of the FRC for appropriately independent oversight of this monitoring process which should publish an engagement survey on an annual basis.

Recommendation 19 Fund managers and other institutions authorised by the FSA to undertake investment business should signify on their websites or in another accessible form whether they commit to the Stewardship Code. Disclosure of such commitment should be accompanied by an indication whether their mandates from life assurance, pension fund and other major clients normally include provisions in support of engagement activity and of their engagement policies on discharge of the responsibilities set out in the Stewardship Code. Where a fund manager or institutional investor is not ready to commit and to report in this sense, it should provide, similarly on the website, a clear explanation of its alternative business model and the reasons for the position it is taking.

Recommendation 20 The FSA should require institutions that are authorised to manage assets for others to disclose clearly on their websites or in other accessible form the nature of their commitment to the Stewardship Code or their alternative business model.

Recommendation 20B In view of the importance of facilitating enhanced engagement between shareholders and investee companies, the FSA, in consultation with the FRC and Takeover Panel, should keep under review the adequacy of the what is in effect "safe harbour" interpretation and guidance that has been provided as a means of minimising regulatory impediments to such engagement.

Recommendation 21 Institutional investors and fund managers should actively seek opportunities for collective engagement where this has the potential to enhance their ownership influence in promoting sustainable improvement in the performance of their investee companies. Initiative should be taken by the FRC and major UK fund managers and institutional investors to invite potentially interested major foreign institutional investors, such as sovereign wealth funds, public sector pension funds and endowments, to commit to the Stewardship Code and its provisions on collective engagement.

Recommendation 22 Voting powers should be exercised, fund managers and other institutional investors should disclose their voting record, and their policies in respect of voting should be described in statements on their websites or in another publicly accessible form.

Governance of risk

Recommendation 23 The board of a FTSE 100-listed bank or life insurance company should establish a board risk committee separately from the audit committee. The board risk committee should have responsibility for oversight and advice to the board on the current risk exposures of the entity and future risk strategy, including strategy for capital and liquidity management, and the embedding and maintenance throughout the entity of a supportive culture in relation to the management of risk alongside established prescriptive rules and procedures. In preparing advice to the board on its overall risk appetite, tolerance and strategy, the board risk committee should ensure that account has been taken of the current and prospective macroeconomic and financial environment drawing on financial stability assessments such as those published by the Bank of England, the FSA and other authoritative sources that may be relevant for the risk policies of the firm.

Recommendation 24 In support of board-level risk governance, a BOFI board should be served by a CRO who should participate in the risk management and oversight process at the highest level on an enterprise-wide basis and have a status of total independence from individual business units. Alongside an internal reporting line to the CEO or CFO, the CRO should report to the board risk committee, with direct access to the chairman of the committee in the event of need. The tenure and independence of the CRO should be underpinned by a provision that removal from office would require the prior agreement of the board. The remuneration of the CRO should be subject to approval by the chairman or chairman of the board remuneration committee.

Recommendation 25 The board risk committee should be attentive to the potential added value from seeking external input to its work as a means of taking full account of relevant experience elsewhere and in challenging its analysis and assessment.

Recommendation 26 In respect of a proposed strategic transaction involving acquisition or disposal, it should as a matter of good practice be for the board risk committee in advising the board to ensure that a due diligence appraisal of the proposition is undertaken, focussing in particular on risk aspects and implications for the risk appetite and tolerance of the entity, drawing on independent external advice where appropriate and available, before the board takes a decision whether to proceed.

Recommendation 27 The board risk committee (or board) risk report should be included as a separate report within the annual report and accounts. The report should describe thematically the strategy of the entity in a risk management context, including information on the key risk exposures inherent in the strategy, the associated risk appetite and tolerance and how the actual risk appetite is assessed over time covering both banking and trading book exposures and the effectiveness of the risk management process over such exposures. The report should also provide at least high-level information on the scope and outcome of the stress-testing programme. An indication should be given of the membership of the committee, of the frequency of its meetings, whether external advice was taken and, if so, its source.

Remuneration

Recommendation 28 The remuneration committee should have a sufficient understanding of the company's approach to pay and employment conditions to ensure that it is adopting a

coherent approach to remuneration in respect of all employees. The terms of reference of the remuneration committee should accordingly include responsibility for setting the over-arching principles and parameters of remuneration policy on a firm-wide basis.

Recommendation 29 The terms of reference of the remuneration committee should be extended to oversight of remuneration policy and outcomes in respect of all "high end" employees.

Recommendation 30 In relation to "high end" employees, the remuneration committee report should confirm that the committee is satisfied with the way in which performance objectives and risk adjustments are reflected in the compensation structures for this group and explain the principles underlying the performance objectives, risk adjustments and the related compensation structure if these differ from those for executive board members.

Recommendation 31 For FTSE 100-listed banks and comparable unlisted entities such as the largest building societies, the remuneration committee report for the 2010 year of account and thereafter should disclose in bands the number of "high end" employees, including executive board members, whose total expected remuneration in respect of the reported year is in a range of £1 million to £2.5 million, in a range of £2.5 million to £5 million and in £5 million bands thereafter and, within each band, the main elements of salary, cash bonus, deferred shares, performance-related long-term awards and pension contribution. Such disclosures should be accompanied by an indication to the extent possible of the areas of business activity to which these higher bands of remuneration relate.

Recommendation 32 FSA-authorised banks that are UK-domiciled subsidiaries of non-resident entities should disclose for the 2010 year of account and thereafter details of total remuneration bands (including remuneration received outside the UK) and the principal elements within such remuneration for their "high end" employees on a comparable basis and timescale to that required for UK-listed banks.

Recommendation 33 Deferral of incentive payments should provide the primary risk adjustment mechanism to align rewards with sustainable performance for executive board members and "high end" employees in a BOFI included within the scope of the FSA Remuneration Code. Incentives should be balanced so that at least one-half of variable remuneration offered in respect of a financial year is in the form of a long-term incentive scheme with vesting subject to a performance condition with half of the award vesting after not less than three years and of the remainder after five years. Short-term bonus awards should be paid over a three-year period with not more than one-third in the first year. Clawback should be used as the means to reclaim amounts in circumstances of misstatement and misconduct. This recommended structure should be incorporated in the FSA Remuneration Code review process next year and the remuneration committee report for 2010 and thereafter should indicate on a "comply or explain" basis the conformity of an entity's "high end" remuneration arrangements with this recommended structure.

Recommendation 34 Executive board members and "high end" employees should be expected to maintain a shareholding or retain a portion of vested awards in an amount in line with their total compensation on a historic or expected basis, to be built up over a period at the discretion of the remuneration committee. Vesting of stock for this group should not normally be accelerated on cessation of employment other than on compassionate grounds.

Recommendation 35 The remuneration committee should seek advice from the board risk committee on specific risk adjustments to be applied to performance objectives set in the context of incentive packages; in the event of any difference of view, appropriate risk adjustments should be decided by the chairman and NEDs on the board.

Recommendation 36 If the non-binding resolution on a remuneration committee report attracts less than 75 per cent of the total votes cast, the chairman of the committee should stand for re-election in the following year irrespective of his or her normal appointment term.

Recommendation 37 The remuneration committee report should state whether any executive board member or "high end" employee has the right or opportunity to receive enhanced benefits, whether while in continued employment or on termination, resignation, retirement or in the wake of any other event such as a change of control, beyond those already disclosed in the directors' remuneration report and whether the committee has exercised its discretion during the year to enhance such benefits either generally or for any member of this group.

Recommendation 38/39 Remuneration consultants should put in place a formal constitution for the professional group that has now been formed, with provision: for independent oversight and review of the remuneration consultants code; that this code and an indication of those committed to it should be lodged on the FRC website; and that all remuneration committees should use the code as the basis for determining the contractual terms of engagement of their advisers; and that the remuneration committee report should indicate the source of consultancy advice and whether the consultant has any other advisory engagement with the company.[160]

Over in the US there has been a concerted effort to strengthen corporate governance for US publicly traded companies, based around important sets of principles as one such version demonstrates:

> I. Board Responsibility for Governance: Governance structures and practices should be designed by the board to position the board to fulfil its duties effectively and efficiently.
>
> II. Corporate Governance Transparency: Governance structures and practices should be transparent – and transparency is more important than strictly following any particular set of best practice recommendations.
>
> III. Director Competency & Commitment: Governance structures and practices should be designed to ensure the competency and commitment of directors.
>
> IV. Board Accountability & Objectivity: Governance structures and practices should be designed to ensure the accountability of the board to shareholders and the objectivity of board decisions.
>
> V. Independent Board Leadership: Governance structures and practices should be designed to provide some form of leadership for the board distinct from management.
>
> VI. Integrity, Ethics & Responsibility: Governance structures and practices should be designed to promote an appropriate corporate culture of integrity, ethics, and corporate social responsibility.
>
> VII. Attention to Information, Agenda & Strategy: Governance structures and practices should be designed to support the board in determining its own priorities, resultant agenda, and information needs and to assist the board in focusing on strategy (and associated risks).
>
> VIII. Protection Against Board Entrenchment: Governance structures and practices should encourage the board to refresh itself.

> IX. Shareholder Input in Director Selection: Governance structures and practices should be designed to encourage meaningful shareholder involvement in the selection of directors.
>
> X. Shareholder Communications: Governance structures and practices should be designed to encourage communication with shareholders.[162]

There is a widely held view that we do not need more regulation, but we need better regulation. The trend to requiring more levels of disclosure looks good on paper, but the excessive amounts of information could cloud annual reports and make them even more confusing. The Financial Reporting Council have indicated that more information does not always make for clearer information:

> One widely acknowledged problem is that reports currently aim to please too many types of user. There is a need to refocus them on their primary purpose: providing investors with information that is useful for making their resource allocation decisions and assessing management's stewardship. We suggest that regulators and companies should reconsider how they address the needs of other stakeholders – for example, those with specialist interests in environmental and employee diversity issues.[163]

Transparency underpins good governance and companies are starting to report big picture issues as well as the detailed commentary that appears in the increasingly long and cumbersome annual reports. The Financial Reporting Council has developed four principles for effective communication when developing reports that are set out as follows:

> The lessons learned from the UK ASB's work on the Operating and Financial Review (OFR) should be extended to cover corporate reporting in its entirety. Reports should be:
>
> 1. **Focused:** Highlight important messages, transactions and accounting policies and avoid distracting readers with immaterial clutter.
> 2. **Open and honest:** Provide a balanced explanation of the results – the good news and the bad.
> 3. **Clear and understandable:** Use plain language, only well defined technical terms, consistent terminology and an easy-to-follow structure.
> 4. **Interesting and engaging:** Get the point across with a report that holds the reader's attention.[164]

One issue that is starting to hit the corporate agenda is the need to ensure that the governance machine is driven by sound business ethics. There is little point viewing regulatory requirements as burdens on large companies that need to be "got around" whenever possible. Ethical governance is based more on wanting to be transparent to shareholders rather than grudgingly adhering to the rules. Moreover, sound internal controls are seen as good business over and beyond a mere compliance reporting requirements that does not have much business value. Corporate transparency is about inviting EA to review the accounts and looking forward to their opinion and any ideas they may have to strengthen financial reporting controls. For IA, this positive view is so important. It means being invited to the top table, rather than listening in at the door.

When we think of corporate governance, we immediately think about the huge multinational companies and the large government bodies that have a profound impact on the economy and society in general. Richard Todd has written a paper for the Handbook that addresses the need to consider the very same corporate governance requirements for smaller organizations that traditionally do not have an internal audit presence.

Corporate Governance in Small Organisations – by Richard Todd

In the recent past it is clear that there has become a greater need for transparency and accountability in smaller organisations, in particular the voluntary sector. Traditionally these areas have limited experience of management or financial control. These organisations are characterised by their honest belief in delivering a service in the chosen area of expertise, but when it comes to governance and control there can be little doubt that internal control takes a poor second place if it exists at all. Small business represents a new area for Internal Auditors to flourish in. Traditionally the Internal Audit function was limited to the larger enterprises, and the Public Sector. This is no longer the case. The ethos of Corporate Governance calls more and more for transparency and control. Government departments providing grant funding to the voluntary sector want to be assured that the funds have been appropriated in a prescribed manner in line with the grant conditions. The role of the Internal Auditor is continually changing; the knowledge, skills and disciplines of the Internal Auditor could be vital to small organisations. This role is not just in terms of reviewing systems, quite the contrary; rather it is to give advice on the strategic direction in terms of managing risk and planning controls. Planning is the key to success.

Small organisations by their very nature do not tend to give an awful lot of time to addressing the thorny issue of risk, internal control and Corporate Governance. Small organisations are often focused on delivering their services to the consumer and therefore maximizing profits. Corporate Governance to a small entity is sometimes not seen as germane to the existence of the organisation, and as a result is de-prioritised. I must say that this view is a fallacy. Corporate Governance in the short term may well reduce profits but in the longer term it will serve to strengthen control within the organisation and promote greater profits. Recently we have seen a spate of small charitable organisations finding themselves in trouble with Government agencies in terms of the appropriateness of their expenditure.

Common Mistakes: Lack of effective stewardship: Stewardship is where there is no clear distinction between who is developing and implementing the strategic direction. In some cases the people developing strategy at board or trustee level are the same individuals conducting the day-to-day functions. Corporate Governance calls for a separation of the day-to-day responsibility from the setting of strategic direction. This is a blurred area for small voluntary organisations. The decision-making process in some voluntary organisations is not clear. I have seen some organisations where operation staff make strategic decisions without it being fully considered by the board. This is a particular concern where operations are geographically spread and where staff have an element of local autonomy. Again this is where it is of the utmost importance to set out the following:

- Lack of documented procedures. Very often small voluntary organisations don't have documented procedures. Again this is a failing of the board or trustees, in that they are charged with the responsibility of ensuring that there are effective procedures within the organisation. In a recent talk I gave to church trustees I asked if they had documented procedures, to which they replied, no. They felt is was superfluous as all staff were experienced and knew instinctively what they were doing. The issue here is not whether or not staff know what they are doing, rather it is to give management some assurance that staff and operatives are discharging their day-to-day responsibilities in a prescribed manner; furthermore, documented procedures lend themselves to ongoing reviews. This indeed strikes at the heart of Corporate Governance. How can the board or trustees be assured of the integrity of operations under their control if they don't know or are unsure of the day-to-day operations. If the board issues documented

procedures then it follows that they are thus aware of the procedures. The other side of the coin is that staff have clear guidance and direction on how to discharge their day-to-day responsibilities. Documented procedures are a key internal control per se. As obvious as it may sound, to get voluntary organisations to document procedures can be a cumbersome task. Once documented procedures are in place the next step would invariably be to ensure that such procedures are complied with. Again this is where internal audit has a review role.

- Lack of internal control. One characteristic of voluntary organisations is the amount of trust placed on individuals. A general response I get from organisations when asked about the omission of key controls is 'we trust our staff'. In my experience the term 'trust' in a corporate sense is a euphemism for lack of internal controls. This is particularly poignant in faith-based organisations, where the essence of the organisation is based on absolute trust. The nature of small enterprises does not lend itself to effective internal control. Hence, poor financial and budgetary controls can undermine the effectiveness of the organisation in delivering the service and thus achieving its stated objectives.
- A culture of non-accountability. Voluntary organisations can be lax in the way they manage their financial and operational systems. Where this has gone on for years without challenge it becomes endemic in the very culture of the organisation. To effect this in anyway and change it is a massive undertaking. Recently I gave a talk to church leaders and trustees, the aim of the talk was to draw attention to the need for effective management control and transparency. They wanted to ensure that all sections of the church were accountable to the trustees, and what better way to do this than to call in an independent consultant to reinforce the point. Accountability is the linchpin of Corporate Governance.

Good Practice: For voluntary organisations or even small businesses in general they must embrace the concept of Corporate Governance, the awarding of Government contracts and grant funding may well depend on it, inter alia. I view Corporate Governance in practical terms, as a jigsaw puzzle, where each piece when fitted together provides the whole picture. Outlined below are the areas which must be included in the governance process:

1. Management body composition and structure.
2. Financial accounting and budget control arrangements.
3. Assets, insurance and security.
4. Banking arrangements.
5. Income control.
6. Personnel.

Management Body. The management body can be the Board, Trustees or Committee, whatever the title from a governance perspective it is a Governing Body. The Governing Body is charged with the determination of strategic policies and controls. Members of the Governing Body should not have any day-to-day involvement in the operations of the organisation. This very often is an area that is blurred in small entities. It is my experience that this is an area that Internal Audit must be mindful of when reviewing such organisations. The Governing Body will delegate day-to-day responsibilities to a named member of staff. The Governing Body will decide what quorum is required as a prerequisite to decision making, and a timetable for Governing Body meetings. Further the Governing Body may set up other committees to deal with personnel and or financial matters along with a certain level of delegated responsibility.

Financial Accounting Budget Control Arrangements. Financial control is a key area within any business entity. To this end the Governing Body will invariable set up a finance committee to

oversee this, and will report to the Governing Body periodically. This is an area that attracts the most Internal Audit attention. Areas of concern will include:

1. Are the accounting arrangements sound?.
2. Is there effective budget monitoring?.
3. Are financial procedures documented and are they complied with?.
4. Revenue and capital expenditure control?

Asset Control, Insurances and Security. The Governing Body will make appropriate arrangements for the safe custody of stocks, stores, furniture and property. This will include asset registers, stock inventory records, custody of property deeds, etc. It is the Governing body's responsibility to safeguard assets and they will have to direct staff in such a way as to reinforce this. Where the organisation has assets, which are in excess of a de minimis value as set by the Governing Body, such assets should be insured. It is perhaps worth remembering at this point that data is an asset and as such it too has to be safeguarded against loss, damage or theft. Security over assets will manifest itself in various forms. Property must be physically protected, furniture and stock items where possible must be security marked and housed in a secure area. Systems data must be access via password control, and there must be effective back-up of all data.

Banking Arrangements. This should go without saying but I will say it anyway. All bank accounts are to be held in the organisation's name, and none are to be registered in the names of individuals. Bank mandates and the Governing Body must determine signatories. Listed below are the key areas to be controlled:

1. Bank mandate should be held securely.
2. Bank statement should be received monthly and reconciled.
3. All takings must be banked intact.

Control over Income. All income to the organisation should be entered in source records at the earliest opportunity. Systems must be in place to ensure that debtors are identified and recorded in the organisation's books of account in a timely fashion. The Governing Body must ensure that there is an effective debt management policy in existence, which sets out clearly how debt is to be pursued. Other income such as donations, etc. must be recorded and banked periodically.

Personnel. No organisation can exist without people to run it. It is inherent therefore for the Governing Body to recognize this and have policies in place to attract, train, develop and retain staff. I won't go into detail on personnel matters, but staff are assets to the organisation, although it is not recorded as such in the books of account, and in the same way as other assets the Governing Body needs to safeguard them.

I heard it once said that business is not for the swift but for those who can endure it. This is true of governance in the voluntary sector. Those organisations that take time to embrace it will in the longer-term benefit from it. On the other hand those that don't address governance in a systematic way could undermine the aims and objectives of the organisation for which they are charged with managing. In my experience, organisations which embrace governance at the outset, move from strength to strength. In this day and age government departments are sceptical about doing business with voluntary or charitable organisations without evidence of strong Corporate Governance. There is an ever greater need to ensure that any government funds are appropriated in a prescribed manner with conditions set by the funding body.

Summary and Conclusions

The corporate governance debate is ongoing. The various codes and guidance that have been prepared throughout the world tend to build on what is already available. New codes have the advantage of recent information on what is working well and where there are still problems matching the theory with real life. As soon as we present the latest position on codes of practice, they are overtaken by a new version which is more inclusive and generally more comprehensive. International codes are coming together to form a common understanding of how corporate, commercial and public life should be conducted. The tremendous pressures inherent in environmental groups and global activists place the conduct of large organizations in the spotlight where people are beginning to define acceptable and unacceptable corporate behaviours. The fully built model of corporate governance that we have been developing in this chapter is set out in Figure 2.11.

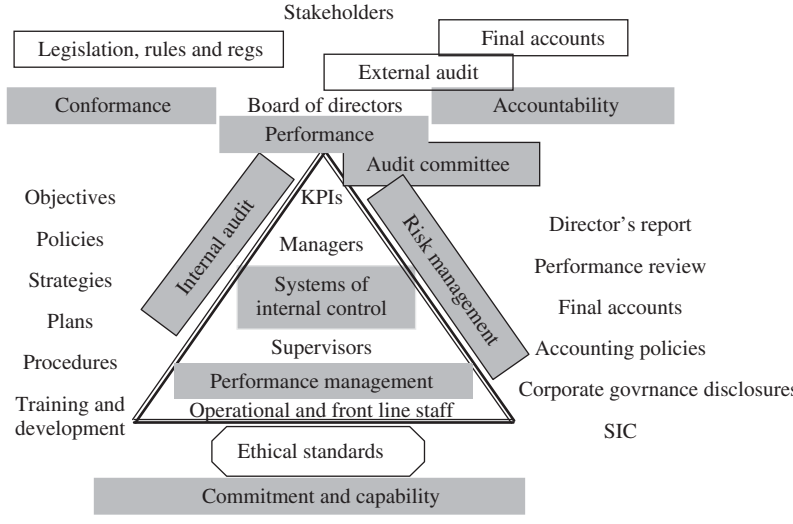


FIGURE 2.11 Corporate governance (7).

Many of the components of our model have already been referred to, but for completeness we can list them all and spend a little more time on the new additions:

- **Stakeholders –** should understand the role of the organization and what they get from it, and be discerning in demanding information on the system of corporate governance in place.
- **Legislation, rules and regulations –** these should all contribute to protecting people and groups who have invested in the organization or who have a direct interest in either the services or products provided or any partnering arrangements. The regulatory framework should also ensure a level playing field for competitors and inspire substance over form.
- **Final accounts –** the annual report and accounts should contain all the information that is required by users and be presented in a true and fair manner (in conjunction with international accounting standards). It should act as a window between the outside world and the organization so that interested users can peer through this window and get a clear view of

the way management behave and their performance, with no chance of skeletons being hidden in the closet.

- **External audit –** there should be a truly independent, competent and rigorous review of the final accounts before they are published, without the distraction of the need to attract large amounts of non-audit fees from the company in question.
- **The board –** the board should be a mix of executives and non-executives balanced so as to represent the interests of the shareholders in a professional and responsible manner, chaired by a respected NED. Their responsibilities should be fully defined and assessment criteria should be in place that ensure fair rewards are available for effective performance (via a remunerations committee).
- **Audit committee –** this committee of non-executives should provide an oversight of the corporate governance process and have a direct line to the shareholders via a separate report in the annual report. The committee should also seek to ensure management are equipped to install effective risk management and controls in the organization. Competent and experienced people should sit on the committee and ensure they are able to commit sufficient time and effort to the task of guiding and monitoring the accounting, audit, accountability, ethical values and governance arrangements, with no conflicts of interest – real or perceived.
- **Performance, conformance and accountability –** these three concepts should form a framework for corporate behaviour where the spirit of the ideals are embraced (as part of organizational culture) in contrast to a list of rules that are studied by legal and accounting technicians with a view to 'getting around'.
- **Key performance indicators (KPIs) –** organizational effort should be formed around a clear mission, vision and set of values that fall into a balanced range of performance measures that ensure risks to effective performance are understood and properly managed.
- **Internal audit –** should be professional, independent and resourced to perform to the professional standards enshrined in the new focus on risk management, control and governance; with a good balance of assurance and consulting effort.
- **Risk management –** there should be a robust system of risk management in place that is embedded into the organizational systems and processes and which feeds into an assurance reporting system (normally based on risk registers).
- **Managers, supervisors and operational and front line staff –** should all understand the corporate governance framework and live up to the demands of their defined responsibilities (for performance, conformance and accountability) in this respect.
- **Systems of internal control –** should exist throughout the organization and be updated to take account of all material risks that have been assessed, and should be owned and reviewed by the people who are closest to the associated operations. The published annual report should comment on the systems of internal control in place to manage internal and external risk.
- **Performance management –** the response to corporate governance ideals should be fully integrated into the way people set targets and assessed in respect of their performance against these targets. Performance should be measured and managed in a balanced and meaningful manner.
- **Ethical standards –** should form the platform for all organizational activities and should be given priority for all-important decisions that are made. They should also underpin the human resource management systems (e.g. selection, training, appraisal, disciplinary, etc.) and be part of clear and consistent messages and values from top management. All employees should be encouraged to report all actual and potential risks to the business, customers and stakeholders, and positive action should be taken by management as a result.

- **Commitment and capability –** are two further concepts that have been added to performance, conformance and accountability. Commitment is the embodiment of corporate governance values into the hearts and minds of everyone connected with the organization. Capability relates to the training, budgets, time and understanding that are needed to make any new arrangements, such as control self-assessment, work. There are many organizations who send bold statements on the need for, say, better risk management but then fail to provide training, resources or space to enable people to do something about any gaps. Performance, conformance, accountability, commitment and capability are the key drivers for ensuring an enthusiastic response to corporate governance.

The need to maintain public confidence in the corporate sector and credibility in government and not-for-profit sectors has never been stronger. There are calls from all quarters to maintain this pressure to improve, develop and progress corporate governance arrangements as far as possible.

Chapter 2: Assignment Questions

Having worked through the chapter, the following questions may be attempted (see Appendix A). Note that the question number relates to the section of the chapter that contains the relevant material.

1. Explain the agency concept and discuss why is it important to secure accountability in companies where ownership is separated from management.
2. Describe why a corporate code of ethics is important and list some of the matters that may be covered in a typical code.
3. Outline two well-known scandals that have demonstrated the need for proper corporate governance and suggest reasons why these problems have occurred.
4. Discuss the concept of corporate governance and describe some of the issues that are addressed in international stock exchanges (and public sector) codes.
5. Describe the matters that organizations are reporting in their published annual corporate governance statements and suggest ways that these reports can be improved.
6. Describe the role of external audit and explain the difference between the external and internal auditing roles.
7. Discuss why audit committees are becoming popular and describe the areas that may fall under the remit of the audit committee.
8. Explain how internal audit fits into the corporate governance equation, and outline what the corporate governance codes say about the value from internal audit.
9. Describe the links between corporate governance, risk management and internal control.
10. Prepare a presentation to the board on the importance of preparing a robust statement on the organization's system of internal control for the published annual report.

Chapter 2: Multi-choice Questions

2.1 Which is the most appropriate statement?

a. Corporate Governance has been described by Adrian Cadbury as the way organizations are directed or controlled.
b. Corporate Governance has been described by Adrian Cadbury as the way organizations are directed and controlled.
c. Corporate Governance has been described by Adrian Cadbury as the way larger organizations are directed and controlled.

d. Corporate Governance has been described by Adrian Cadbury as the way organizations are risk assessed and controlled.

2.2 Insert the missing phrase:

a. Corporate governance codes and policies have come to be relied on to re-establish the performance/conformance balance to ensure .....

a. integrity, openness and responsibility
b. integrity, fair play and accountability
c. integrity, honesty and accountability
d. integrity, openness and accountability

2.3 Which is the most appropriate statement?

a. The directors formulate a corporate strategy to achieve set objectives and meet customers' expectations, and in turn, employ managers and staff to implement this strategy.
b. The directors formulate a corporate strategy to achieve set objectives and meet market expectations, and in turn, employ a board of directors to implement this strategy.
c. The shareholders formulate a corporate strategy to achieve set objectives and meet market expectations, and in turn, employ managers and staff to implement this strategy.
d. The directors formulate a corporate strategy to achieve set objectives and meet market expectations, and in turn, employ managers and staff to implement this strategy.

2.4 Insert the missing phrase:

a. All business activity feeds into the accounting system and the directors report the results back to their ..... in the annual report on performance and accompanying final accounts.

a. audit committee
b. shareholders
c. bankers
d. auditors

2.5 Which is the most appropriate statement?

a. The Stewardship concept means directors owe this responsibility to the parties who have a vested interest in the organization. They work for and on behalf of their masters, and need to demonstrate competence, which is not always easy.
b. The Stewardship concept means directors owe this responsibility to the parties who work for the organization. They work for and on behalf of their masters, and need to demonstrate competence, which is not always easy.
c. The Stewardship concept means directors owe this responsibility to the parties who have a vested interest in the organization. They work for and on behalf of their masters, and need to demonstrate helpfulness, which is not always easy.
d. The Stewardship concept means directors owe this responsibility to the parties who have a vested interest in the organization. They work for and on behalf of the regulators, and need to demonstrate competence, which is not always easy.

2.6 Insert the missing phrase:

a. For public bodies, the owners are the taxpayers and the external auditors have an additional role in ..... as well as verifying the financial statements.

a. assessing performance
b. assessing value for money (VFM)
c. assessing performance and value for money (VFM)
d. assessing ethics, performance and value for money (VFM)

2.7 For central government organizations, the responsible person in terms of corporate governance reporting is .....
   a. the chief executive
   b. the accounting officer
   c. the principle officer
   d. the reporting officer

2.8 Which is the most appropriate statement?
   a. In general there are two types of stakeholders; those that have a direct *influence* on the organization's future activities such as journalists, regulators and shareholders; and those that simply have an *interest* in the organization, such as local community groups and customers.
   b. In general there are two types of stakeholders; those that have a direct *influence* on the organization's future activities such as investors, customers and shareholders; and those that simply have an *interest* in the organization, such as regulators, local community groups and journalists.
   c. In general there are two types of stakeholders; those that have a direct *influence* on the organization's future activities such as investors, customers, regulators and shareholders; and those that simply have an *interest* in the organization, such as local community groups, and journalists.
   d. In general there are two types of stakeholders; those that have a direct *influence* on the organization's future activities such as investors, customers, regulators; and those that simply have an *interest* in the organization, such as shareholders, local community groups, and journalists.

2.9 Which is the odd one out?
The Nolan Principles on standards in public life comprise the following:
   a. Selflessness
   b. Integrity
   c. Objectivity
   d. Accountability
   e. Openness
   f. Justice
   g. Honesty
   h. Leadership

2.10 The late Anita Roddick, from the Body Shop has suggested that:

> I would love it if every shareholder of every company wrote a letter every time they received a company's annual report and accounts. I would like them to say something like "Okay that's fine, very good. But where are the details of your environmental audit? Where are your details of accounting to the community? Where is your ..... ?"

   a. audit team
   b. audit committee
   c. audit programme
   d. social audit

2.11 Which is the most appropriate statement?
   a. The Public Interest Disclosure Act 1998 applies to England, Scotland and Wales. Disclosures relate to crimes, breaches of legal obligations, miscarriage of justice, inefficient budgeting or the environment and concealing information relating to these items.
   b. The Public Interest Disclosure Act 1998 applies to England, Scotland and Wales. Disclosures relate to crimes, breaches of legal obligations, miscarriage of justice, dangers

to health and safety or the environment and concealing information relating to these items.

c. The Public Interest Disclosure Act 1998 applies to England and Wales. Disclosures relate to crimes, breaches of legal obligations, miscarriage of justice, dangers to health and safety or the environment and concealing information relating to these items.

d. The Public Interest Disclosure Act 1998 applies to England, Scotland and Wales. Disclosures relate to bullying, breaches of legal obligations, miscarriage of justice, dangers to health and safety or the environment and concealing information relating to these items.

2.12 Insert the missing phrase:

a. Sir Adrian Cadbury has said: The country's ..... depends on the drive and efficiency of its companies.

a. society
b. economy
c. success
d. reputation

2.13 Which is the most appropriate statement?

a. Enron collapsed because of its complicated trading activities, and staff manipulation.
b. Enron collapsed because of its complicated market conditions, and financial manipulation.
c. Enron collapsed because of its complicated trading activities, and financial efficiency.
d. Enron collapsed because of its complicated trading activities, and financial manipulation.

2.14 Which is the most appropriate statement?

a. Companies listed on various international stock markets are meant to subscribe to listing rules and must observe the rules.
b. Companies listed on various international stock markets are meant to subscribe to listing rules or make clear their reasons (and the implications) for failing to observe the rules.
c. Companies listed on various international stock markets are meant to subscribe to listing rules or make clear their reasons for failing to observe the rules.
d. Companies listed on various international stock markets are meant to subscribe to legal provisions or make clear their reasons (and the implications) for failing to observe the rules.

2.15 Which is the odd one out?

Cadbury has described the underpinning principles behind the code:

a. Openness
b. Integrity
c. Decency
d. Accountability

2.16 Which two of the selected extracts from the Turnbull report is wrongly stated?

a. Principle D2; The board should maintain a sound system of internal control to safeguard shareholders' investment and the company's assets.)
b. Principle D2.1; The directors should, at least annually, conduct a review of the effectiveness of the group's system of internal control and should report to shareholders that they have done so. The review should cover all controls, including financial, operational and compliance controls and risk management.
c. Principle D.2.2; Companies which do not have an internal audit function should be required to establish such a function.
d. a narrative statement of how it has applied the principles set out in Section 1 of the Combined Code, providing explanation which enables its shareholders to evaluate how the principles have been applied.

e. a statement as to whether or not it has complied throughout the accounting period with the Code provisions set out in Section 1 of the Combined Code.
f. The intention is that companies should be told how to explain their governance policies in the light of the principles, including any special circumstances which have led them to adopting a particular approach.

2.17 Which is the correct quote from the Cadbury report?
a. The Chief Executive should be able to stand sufficiently back from the day-to-day running of the business to ensure that their boards are in full control of the company's affairs and alert to their obligations to their shareholders.
b. Chairmen should be able to stand sufficiently back from the day-to-day running of the business to ensure that their boards are in full control of the company's affairs and alert to their obligations to their shareholders.
c. Chairmen should be able to stand sufficiently back from the day-to-day running of the business to ensure that their boards are in full control of the company's affairs and alert to their obligations to their chief executives.
d. The Chief Executive should be able to stand sufficiently back from the day-to-day running of the business to ensure that their boards are in full control of the company's affairs and alert to their obligations to their Chairman.

2.18 Insert the missing phrase:
In some European countries such as Germany, the executive board runs the company while the ....., half of whose members are employees, supervises and advises the executive board and is responsible for sensitive areas such as executive board members performance-based remuneration.
a. representative board
b. advisory board
c. supervisory board
d. management board

2.19 Insert the missing phrase:
Coming off the scandals of 2002, by November 2002 the US governance rules were revamped to tighten up on accounting and accountability through the .....
a. Sarbanish-Oxley Act 2002
b. Sarbanes-Oxley Act 2002
c. Sardines-Oxtail Act 2002
d. Sarbailles-Oxley Act 2002

2.20 The External Auditor:
a. Tests the underlying transactions that form the basis of the financial statements. In this way they may form an opinion on whether or not these statements show a true and fair view.
b. Tests the underlying transactions that form the basis of the financial statements. In this way they may ensure that these statements show a true and fair view.
c. Tests the underlying transactions that form the basis of the financial statements. In this way they may form an opinion on whether or not these statements show a true view.
d. Tests the underlying transactions that form the basis of the financial statements. In this way they may state that these statements show a true and fair view.

2.21 Which two of the following statements are wrong in terms of company external auditors?
a. External auditors are generally members of CCAB professional accountancy bodies and are employed under the Companies legislation to audit the accounts of registered companies.

b. They are appointed annually at the annual general meeting by their clients, the shareholders.
c. Their remuneration is fixed by the Director of Finance.
d. They have a right to attend general meetings to discuss any audit-related matters.
e. They have a right of access to all books, information and explanations pertaining to the financial statements.
f. In a limited company they can be removed by ordinary resolution with special notice.
g. They may be officers, corporations or partners or employees of officers.
h. In the event of their resignation they have to provide a statement of circumstances to the new incoming auditor that will document any specific problems with the audit cover.
i. Where there is a problem with the accounts the auditor will fashion a suitable report to reflect the nature of the problem.

2.22 Which is the most appropriate statement?

a. The external auditor seeks to provide an opinion on whether the accounts show a true and fair view. Whereas internal audit forms an opinion on the adequacy and effectiveness of systems of risk management and internal control, which also relates to the main accounting systems.
b. The external auditor seeks to provide an opinion on whether the accounts show a true and fair view. Whereas internal audit forms an opinion on the truth and fairness of systems of risk management and internal control, many of which fall outside the main accounting systems.
c. The external auditor seeks to provide an opinion on whether the accounts show a true and fair view. Whereas internal audit forms an opinion on the adequacy and effectiveness of compliance with internal control, many of which fall outside the main accounting systems.
d. The external auditor seeks to provide an opinion on whether the accounts show a true and fair view. Whereas internal audit forms an opinion on the adequacy and effectiveness of systems of risk management and internal control, many of which fall outside the main accounting systems.

2.23 Insert the missing phrase:

Many problems are caused by differing perceptions by external audit and users of financial statements audited by the external auditors. This is commonly known as the "……."

a. management gap
b. expectations gap
c. generation gap
d. auditor's gap

2.24 Which is the most appropriate statement?

a. The external auditor is expected to display a degree of astonishment when they discover indicators of fraud and abuse that impact the reliability of the financial accounts.
b. The external auditor is expected to display a degree of anxiety and react when they discover indicators of fraud and abuse that impact the reliability of the financial accounts.
c. The external auditor is expected to display cynicism and react when they discover indicators of fraud and abuse that impact the reliability of the financial accounts.
d. The external auditor is expected to display a degree of professional scepticism and react when they discover indicators of fraud and abuse that impact the reliability of the financial accounts.

2.25 Insert the missing phrase:
Groundbreaking work was performed in the USA by the ..... who prepared ten key recommendations on improving the effectiveness of audit committee:
a. Standards Committee
b. Regularity Committee
c. Round Table
d. Blue Ribbon Committee

2.26 Insert the missing phrase:
We have already suggested that a " ..... " approach to corporate governance structures is unrealistic, which is why most codes are both voluntary and fairly general in the way they define set standards. There is still scope to prepare best practice guides, even though they cannot be too specific.
a. substance over form
b. one size fits all
c. common or garden
d. systematic

2.27 Which is the most appropriate statement relating to the Audit Committees?
a. Members are appointed by the board and the audit committee should consist of at least three members (and not more than six) being a mix of Non-Executive and Executive Directors.
b. Members are appointed by the board and the audit committee should consist of at least six members being independent non-executive directors.
c. Members are appointed by the board and the audit committee should consist of at least three members (and not more than six) being independent non-executive directors.
d. Members are appointed by the shareholder and the audit committee should consist of at least three members (and not more than six) being independent non-executive directors.

2.28 Which is the most appropriate statement relating to the Audit Committees?
a. Audit Committee meetings should be held at least four times a year and all members should attend unless there are exceptional circumstances.
b. Audit Committee meetings should be held at least three times a year and all members should attend.
c. Audit Committee meetings should be held at least three times a year and all members should attend unless there are exceptional circumstances.
d. Audit Committee meetings should be held at least ten times a year and all members should attend unless there are exceptional circumstances.

2.29 Insert the missing word:
The Smith Report suggests that at least one member of the audit committee should have significant, recent and relevant ..... experience.
a. operational
b. industry specific
c. audit committee
d. financial

2.30 Which is the most appropriate statement?
a. Moreover the internal auditor can be the best friend of the audit committee and is one of the many parties that can be relied on to give impartial and reliable advice and information.
b. Moreover the internal auditor can set up the audit committee and is perhaps one of the few parties that can be relied on to give impartial and reliable advice and information.

c. Moreover the internal auditor can be the best friend of the audit committee and is perhaps one of the few parties that can be relied on to give impartial and reliable advice and information.
d. Moreover the internal auditor sits on the audit committee and is one of the many parties that can be relied on to give impartial and reliable advice and information.

2.31 Insert the missing word:
If controls drive the organization forward and also tackle all known ..... that threaten this positive direction, then there is a good system of internal control in place.
a. risks
b. external factors
c. occurrences
d. persons

References

1. *The Irish Times*, Tiarnan O'Mahoney, (www.ireland.com, 21 Nov. 2001).
2. *Daily Mail*, 30 Mar. 1996, p. 14.
3. Andrew Tonge 'Keeping better company'. *Accountancy Age*, 23 April 1999, pp. 16–17.
4. 'Rearranging the board'. *Internal Auditing and Business Risk*, April 2002, pp. 28–29.
5. Andrew Chambers (2002) 'Stakeholders – the court of public opinion' *Corporate Governance Handbook*: Tolley's, Reed Elsevier (UK) Ltd, p. 627.
6. The Institute of Directors, (www.iod.co.uk).
7. Telecomasia Corporation Public Co. Ltd, Annual Report 2000 (www.telecomasia.net).
8. 1999–2002 BP PLC. (www.bp.com).
9. *Daily Mail*, 17 Jan. 2002, p. 75, 'Tough guy rough is a hard act to follow' (David Rough), City and Finance, The City Interview by Feltham Cliff.
10. *Evening Standard*, Friday 22 Mar. 2002, p. 73, Business Day, 'Dark secrets of the boardroom bonus pay plans', Anthony Hilton.
11. Mathew Weait 'The workplace ethic – is it a crime'. *Management Today*, Jan. 2001, pp. 53–55.
12. *Daily Mail*, Tuesday 23 Jan. 2001, p. 7, 'Customers' revenge', James Tozer.
13. The Reith Lectures BBC (www.bbc.co.uk).
14. Nick Edwards 'Whose ethics?' *Supply Management*, 3 Oct. 1996, pp. 20–21.
15. *Daily Mail*, Wednesday 8 Dec. 1999, p. 3, 'Model agency bans under-16 girls after TV sex scandal', Lisa O'Carroll and Rick Hewett.
16. *Daily Mail*, Wednesday 22 May 2002, p. 77, City and Finance, 'Tips row costs Merrill £70m', Sunderland Ruth.
17. Stilltow John *Internal Auditing*, May 1999, pp. 12–13.
18. Ian Jones and Michael Pollitt (eds) (1998) 'The role of business ethics in income performance', *The Role of Voluntary Codes of Practice in Setting Ethics, Adrian Cadbury*: Macmillan Press Ltd, p. 68.
19. Civil Service Code (www.cabinet-office.gov.uk).
20. *The Times*, 5 Mar. 1999, 'Surgeons still try to cover up errors', Jeremy Laurance.
21. Code of Practice on Openness in the NHS, Ref: 1578 4P 3k Jan. 97(01).
22. The Nolan Code (www.public-standards.gov.uk).
23. Gareth Jones 'Look after your heart'. *People Management*, 29 Jul. 1999, p. 27.
24. Roger Maitland 'Due consideration'. *People Management*, 24 Jan. 2002, p. 51.
25. Mary Harpur Oonagh Chief Executive of the IOD, 'Promoting enterprise with integrity'. *Internal Auditing*, Feb. 2000, p. 6.
26. www.transparency.org.
27. www.oecd.org.
28. United Nations, Department of Technical Co-operation and Development, Accounting and Auditing of Foreign Aid Programmes and EDP Audit, Report of the United Nations/Intosai, Expert Group Meeting on Government Auditing, Vienna, 12–21 Sept. 1990.

29. Roger Adams 'A question of ethics'. *Accounting and Business*, Mar. 1999, pp. 4–5.
30. Internal Auditing and Business Risk, Governance Responsibility Reporting, Moon Chris Feb. 2002, pp. 36–37, Association of British Insurers Guidelines on Social, Ethical and Environmental (SEE) Issues – Investing in Social Responsibility – Oct. 2001.
31. Internal Auditing and Business Risk, Governance Responsibility Reporting, Moon Chris Feb. 2002, pp. 36–37, Association of British Insurers Guidelines on Social, Ethical and Environmental (SEE) Issues – Investing in Social Responsibility – Oct. 2001.
32. www.bodyshop.com.
33. www.tesco.co.uk.
34. Neil Baker 'Ready to blow', *Internal Auditing and Business Risk*, Jun. 2002-09-24, pp. 23–25.
35. *Daily Mail*, 23 Nov. 1999.
36. IoD, *Director's Guide to Corporate Social Responsibility*, Lord Newton of Braintree (www.iod.co.uk).
37. 'Corporate governance failures and their impact: in the Institute of Internal Auditors – UK and Ireland Study Text'. *Corporate Governance and Risk Management*, Oct. 2002, p. 17.
38. *Daily Mail*, Friday 28 Nov. 1997, p. 17, 'The £3m backhander Saunders gave himself', David Norris.
39. Lawrence Lever (1992) *The Barlow Clowes Affair*: Macmillan London Ltd, p. 1.
40. Neil Baker and Robert Lea 'A fraud waiting to be detected'. *Accountancy Age*, 27 Apr. 1995, p. 10.
41. 'Corporate governance failures and their impact: in the Institute of Internal Auditors – UK and Ireland Study Text'. *Corporate Governance and Risk Management*, Oct. 2002, p. 18.
42. *Daily Mail*, Saturday 7 April 1996, p. 17, 'Five years jail for fugitive Nadir's Miss Moneypenny'.
43. www.guardian.co.uk/Archive/Article, visited 15/12/2002.
44. 'BCCI man jailed', Court Reporter, *Accountancy Age*, 27 Nov. 1997.
45. www.guardian.co.uk/Archive/Article, visited 15/12/ 2002.
46. 'Corporate governance failures and their impact: in the Institute of Internal Auditors – UK and Ireland Study Text'. *Corporate Governance and Risk Management*, Oct. 2002, p. 18.
47. *Financial Mail on Sunday*, 1 April 2002, p. 10 'Maxwell scandal starts a revolution – auditors face action to end cosy deals with clients' Atkinson Dan and Fluendy Simon.
48. 'Corporate governance failures and their impact: in the Institute of Internal Auditors – UK and Ireland Study Text'. *Corporate Governance and Risk Management*, Oct. 2002, p. 18.
49. www.news.bbc.co.uk, visited 15/12/ 2002.
50. *Evening Standard*, Tuesday 17 Dec. 1996, p. 29 'Lessons learned from Barings amid the confusion', Hilton Anthony, Business Day.
51. Weekes Tim, 'The £5m lesson in swindling'. *Accountancy Age*, 22 June 1995.
52. Weekes Tim, 'The £5m lesson in swindling'. *Accountancy Age*, 22 June 1995.
53. *Daily Mail*, Saturday 15 June 1996, p. 19, 'Fall of King Copper', Burt Jason.
54. www.news.bbc.co.uk/1/hi/business, visited 15/12/ 2002.
55. www.guardian.co.uk/business, visited 15/12/ 2002.
56. www.guardian.co.uk/business, visited 15/12/ 2002.
57. *Financial Mail on Sunday*, 18, Oct. 1998, p. 15, 'Inland Revenue "failures" in corruption case prompt call for whistleblowers' charter – taxman under fire over bribes scandal'.
58. *Financial Mail on Sunday*, 18, Oct. 1998, p. 15, 'Inland Revenue "failures" in corruption case prompt call for whistleblowers' charter – taxman under fire over bribes scandal'.
59. www.news.bbc.co.uk/1/hi/world/Americas, visited 15/12/ 2002.
60. Cooper Cathy 'Management blasted at nuclear plant'. *People Management*, 16 March 2000, p. 16.
61. *Daily Mail*, Wednesday 25 July 2001, p. 41, 'Equitable Life: a sad catalogue of chaos', Hazell Tony and Beugge Charlotte.
62. *Evening Standard*, Friday 15 Nov. 2002, p. 41, 'Equitable Life Is dealt triple blow as crisis deepens', Armstrong Paul and Hilton Anthony.
63. *Daily Mail*, Wednesday 31 Jan. 2001, p. 2, 'Agony of parents in babies scandal', William David and Jenny Hope.
64. 'Corporate governance failures and their impact: in the Institute of Internal Auditors – UK and Ireland Study Text'. *Corporate Governance and Risk Management*, Oct. 2002, p. 19.
65. *Daily Mail*, Thursday 7 Feb. 2002, p. 76, 'Andersen chief caught In the enron crossfire', Laird Laurie. Enron filed for bankruptcy in December 2001.

66. www.news.bbc.co.uk/1/hi/business, visited 15/12/ 2002.
67. *Financial Times*, Thursday 7 Nov. 2002, p. 3, 'Fastow pleads not guilty to 78 Enron charges', McNulty Sheila.
68. *Financial Times*, Friday 20 Dec. 2002, p. 29, 'Ruling on JP Morgan e-mails imminent', Hill Andrew.
69. 'Corporate governance failures and their impact: in the Institute of Internal Auditors – UK and Ireland Study Text', *Corporate Governance and Risk Management*, Oct. 2002, p. 19.
70. www.news.bbc.co.uk, visited 15/12/ 2002.
71. 'Corporate governance failures and their impact: in the Institute of Internal Auditors – UK and Ireland Study Text', *Corporate Governance and Risk Management*, Oct. 2002, p. 19.
72. www.news.bbc.co.uk, visited 15/12/ 2002.
73. www.guardian.co.uk/Business, visited 15/12/ 2002.
74. 'Internal audit needs to act fast if it wants to preserve its credibility after the AIB catastrophe, writes Neil Hodge'. *Internal Auditing and Business Risk*, May 2002, p. 9.
75. www.news.bbc.co.uk/1/hi/business, visited 15/12/ 2002.
76. www.news.bbc.co.uk/1/hi/business, visited 15/12/ 2002.
77. www.news.ft.com/servlet, visited 15/12/ 2002.
78. *Evening Standard*, Thursday 19 Dec. 2002, p. 31, 'CSFB hit by record £4 million FSA fine', Hosking Patrick.
79. www.news.ft.com/servlet, visited 15/12/ 2002.
80. Cadbury Report, 'Report of the Committee on the Financial Aspects of Corporate Governance', 1992, para. 2.5.
81. Cadbury Report, 'Report of the Committee on the Financial Aspects of Corporate Governance', 1992.
82. Rutteman Report, 'Internal control and financial reporting: guidance for directors of listed companies registered in the UK', 1994.
83. The Greenbury Report, 'Directors' remuneration: report of a study group chaired by sir richard greenbury', 1995.
84. Turnbull Report, 'Guidance for Directors on the Combined Code', 1999.
85. Kemeny Lucinda, 'Turnbull faces review'. *Accountancy Age*, 30 Sept. 1999.
86. The Combined Code on Corporate Governance, June 2008, Financial Reporting Council.
87. National Association of Corporate Directors (NACD), Key Agreed Principles to Strengthen Corporate Governance for U.S. Publicly Traded Companies, 16 Oct. 2008,
88. National Health Service, 'Integrated Governance Handbook, a handbook for executives and non-executives in healthcare organisations', Department of Health, Feb. 2006.
89. 'Corporate governance in central government departments: code of good practice', Jul. 2005, HM Treasury, Crown Copyright.
90. Global Principles of Accountable Corporate Governance, Mar. 2009, The California Public Employees' Retirement System (CalPERS).
91. (2007) *Corporate Governance Principle and Recommendations*, 2nd edition: *ASX Corporate Governance Council*.
92. Organisation for Economic Co-Operation and Development, OECD Principles of Corporate Governance, 2004.
93. *21st Century Governance and Financial Reporting Principles*: Corporate Governance Center, Kennesaw State University, 26 Mar. 2002, www.ksumail.kennesaw.edu.
94. Baker Neil, 'The new agenda'. *Internal Auditing and Business Risk*, Aug. 2002, pp. 12–17.
95. Chambers Andrew (2002) 'Stakeholders – the court of public opinion' in *Corporate Governance Handbook*: Tolley's, Reed Elsevier (UK) Ltd., p. 12.
96. GlaxoSmithKline Annual Report 2001 (www.gsk.com, extracts only).
97. Lyttelton Port Company Limited – New Zealand (www.lpc.co.nz, extracts only.)
98. National Archives of Australia Annual Report 2000–01 (www.naa.gov.au, extracts only).
99. Sears Canada Inc, (www.sears.ca, extracts only).
100. Matthey J. M., Annual Report and Accounts 2001 (www.matthey.com, extracts only).
101. BBC Worldwide, (www.bbc.co.uk, extracts only).
102. Reuters Annual Report 1998 (www.reuters.com, extracts only).
103. IoD Factsheets, 8 Jul. 2002, 'What are the responsibilities and liabilities of the directors?' (www.iod.co.uk).
104. IoD Factsheets, 8 July 2002, 'What is the role of the NED?' (www.iod.co.uk).

105. *Daily Mail*, City and Finance, 25 April 2002, p. 69, 'Pension champion who is scourge of fat cats', Sunderland Ruth interviewing Rubenstein Alan.
106. 'Non-executive directors, their value to management'. *CIMA*, Oct. 2001.
107. *ACCA Accounting and Business*, July/Aug. 2001, p. 12.
108. Chambers Andrew, 'Board Osmosis'. *Accounting and Business*, Jun. 1998, p. 41.
109. 'IoD head calls to scrap NEDS' *Internal Auditing and Risk*, Jun. 2002, p. 8.
110. *Financial Times*, Monday 25 Mar. 2002, p. 26, Companies and Finance UK, 'Don't put temptation in the non-execs' way', Plender John.
111. *Evening Standard*, Wednesday 24 April 2002, Business Day (p. 37), 'Why shareholders are suddenly getting restless', Hilton Anthony.
112. IoD Factsheets, 8 July 2002, 'What is the role of the chairman?' (www.iod.co.uk).
113. Sikka Prem 'Power to the people'. *Internal Auditing and Business Risk*, Nov. 2002, p. 10.
114. The 2001/2002 corporate governance survey of corporate Directors, 20 Nov. 2001, Washington, DC.
115. 'Caught in the act, new US governance rules'. *Internal Auditing and Business Risk* – Loose, Nov. 2002, p. 21.
116. New York Stock Exchange, Listing Rules (From: Corporate Governance Rule Proposals Reflecting Recommendations from the New York Stock Exchange Corporate Accountability and Listing Standards Committee, as approved by the NYSE Board of Directors 1 Aug. 2002).
117. Sawers Andrew. *Accountancy Age*, 24 Oct. 1996.
118. Felix William L. Jr, Gramling Audrey A., and Maletta Mario J. 'Internal vs external audit'. *Internal Auditing*, July 1999, pp. 7–9.
119. 'Sharman shakes up public audit'. *Internal Auditing and Business Risk*, Apr. 2001, p. 14.
120. *Internal Auditing and Business Risk*, Apr. 2002, p. 37.
121. 'ICAEW audit and assurance faculty'. *Internal Auditing and Business Risk*, Oct. 2000, p. 21.
122. 'Getting the most out of narrative financial reporting'. Brian Rutherford, *Accounting and Business*, May 2002, pp. 32–33.
123. Hodge Neil 'Quality control'. *Internal Auditing and Business Risk*, Apr. 2002, pp. 21–23.
124. The White Paper, Wells Joe T.
125. *1st Century Governance and Financial Reporting Principles*: Corporate Governance Center, Kennesaw State University, 26 Mar. 2002.
126. Woolfe Emile and Hindson Moria 'Lessons in fraud'. *Accountancy Age* Jul. 2000, p. 128.
127. Chitty David 'No end of a lesson'. *Accountancy*, May 1999, p. 108.
128. *Accountancy Age*, 8 Mar. 2001, p. 14.
129. Australian Shareholders' Association, Media Release – Audit Independence, 25/06/ 2001.
130. Practice Advisory 2030-2: SEC External Auditor Independence Requirements for Providing Internal Audit Services, p. 104.
131. 'Senate slams Enron's "integrated audit", Neil Baker looks at the first outside investigation into the Enron scandal'. *Internal Auditing and Business Risk* – Loose, Aug. 2002, pp. 8–9.
132. Inman Phillip 'Where do we go from here?' *Accountancy Age*, 15 Jan. 1998, p. 16.
133. HM Treasury Dear Accounting Officer Letter 13/00, Annex B, p. 103.
134. Gosling Paul 'Back to front audit'. *Public Finance*, 11–17 Feb. 2000, p. 18.
135. The Audit Commission Code of Practice, Mar. 2002, p. 47, Glossary – Materiality (and Significance).
136. Sharman Lord 'Of Gladstone grab and government'. *Public Finance*, 16–22 Feb. 2001, pp. 21–27.
137. *Evening Standard*, Tuesday 26 Feb. 2002, Business Day (p. 35), Hilton Anthony.
138. John Menzies plc, Annual Report, Extracts – Directors' Responsibilities and Internal Control, (http://www.johnmenziesplc.com/corporate-responsibility/corporate-governance/internal-controls.php#control_environment November 2009).
139. Transport for London (TfL), Annual report 2006 http://www.tfl.gov.uk/corporate/about-tfl/investorrelations/4715.aspx, Nov. 2009.
140. Sports Direct International Plc., Annual Report 2008/09, (http://www.sports-direct-international.com/main.asp?pid=39).
141. HSSA, Annual report 2008/09, (http://www.hsa.gov.sg/publish/etc/medialib/hsa_library/corporate/annual_report_2008.Par.79138.File.dat/corporate_governance_statement.pdf, Nov. 2009).
142. J Sainsbury Plc, Annual Report 2005, (http://www.j-sainsbury.co.uk/ar05/index.asp?pageid=37, Nov. 2009).

143. British American Tobacco p.l.c., Annual Report 2008, Corporate Governance Statement (http://www.bat.com/groupfs/sites/BAT_7NJGCY.nsf/vwPagesWebLive/DO7Q2THL?opendocument&SKN=1 November 2009).
144. The Combined Code on Corporate Governance, Jun. 2008, Financial Reporting Council.
145. Chambers Andrew (2002), *Corporate Governance Handbook*: Tolley's, Reed Elsevier (UK) Ltd, p. 574.
146. Moeller Robert and Witt Herbert (1999) Para. 6.30. *Brink's Modern Internal Auditing*, 5th edition, New York: John Wiley and Sons Inc.
147. Chambers Andrew (2002) *Corporate Governance Handbook*: Tolley's, Reed Elsevier (UK) Ltd, p. 391.
148. Bishop William G. III, Hermanson Dana R., Lapides Paul D., and Rittenberg Larry E. 'Audit committees'. *Internal Auditor*, April 2000, p. 47.
149. Ridley Anthony J. 'An audit committee event matrix'. *Internal Auditor*, April 2000, pp. 14, 53.
150. HMT DAO 13/00, Annex C, Policy Principles for Audit Committees in Central Government.
151. Ridley Jeffrey 'Audit committee, how effective is your audit committee?' *Internal Auditing and Business Risk*, Dec. 2000, p. 30.
152. Rittenberg, Larry *Lessons for Internal Auditors*: Internal Auditor, Apr. 2002, p. 32.
153. www.theiia.org, visited 6 Dec. 2002.
154. Bolton Gill, 'Implementing Turnbull'. *Internal Auditing*, Jun. 2000 (UK), p. 36.
155. IIA. Uk&Ireland – Local Government Auditing In England and Wales, 1998.
156. ZENECA, Directors' Report 1998 (www.astrazeneca.com, extracts).
157. www.nationaltrust.org.uk, National Trust.
158. IIA Global Auditing Information Network, Public reporting on internal controls, flash survey of 414 responses, 4 Apr. 2002 (www.theiia.org).
159. Audit Firm Governance, Evidence Gathering Consultation Paper Issued by the Audit Firm Governance Working Group in a Project for the Financial Reporting Council, 'Comments from ACCA', Jan. 2009.
160. Financial Reporting Council, Louder Than Words 2009, (Principles and actions for making corporate reports less complex and more relevant), p. 20.
161. The Walker Review, A review of corporate governance in UK banks and other financial industry entities, recommendations, 16 Jul. 2009.
162. National Association of Corporate Directors (NACD), Oct. 2008, 'Set of principles to guide corporate leaders as they make boardroom decisions known as the Key Agreed Principles to Strengthen Corporate Governance for U.S. Publicly Traded Companies (Principles)'.
163. Financial Reporting Council, Louder Than Words 2009, (Principles and actions for making corporate reports less complex and more relevant), p. 5.
164. Financial Reporting Council, Louder Than Words 2009, (Principles and actions for making corporate reports less complex and more relevant), p. 7.

Chapter 3

MANAGING RISK

Introduction

The formal definition of internal auditing is repeated here as follows:

> Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.

We need to understand risk and to appreciate the importance of risk management to an organization. Good corporate governance codes require the board to install a system of risk management and tell their shareholders about this system. This chapter addresses the concept of risk. We consider some of the materials that have been written about risk and introduce the risk cycle as a way of understanding how risk management works. We touch on important aspects of the risk-management system relating to risk policies and tools such as enterprise-wide risk management and control self-assessment. The breakthrough into risk has impacted the internal auditor's work and an important account of this move into a new phase of internal auditing was provided in 1998 by David McNamee and Georges Selim, who defined three stages in the development of internal auditing:

1. counting and observing
2. systems of internal control
3. auditing the business process through a focus on risk.

They go on to describe the paradigm shift that enables this leap from stage two to stage three, and argue that:

> The implications of this paradigm shift are enormous. It turns the focus of the audit away from the past and present and toward the present and future. Focusing on controls over transactions buried the internal auditor in the details of the past, limiting the value from any information derived. By focusing on business risks to present and future transactions, the auditor is working at a level above the details and dealing with the obstacles for organisation success. The information derived from such exploration has great value to the management governance team.[1]

The emphasis on risk management now drives many larger organizations, not as a reporting requirement but as a powerful business tool that, used properly, improves performance. Note that all references to IIA definitions, code of ethics, IIA attribute and performance standards,

practice advisories and practice guides relate to the IPPF prepared by the IIA in 2009. In an attempt to get behind risk management, we cover the following ground in this chapter:

3.1 What Is Risk?
3.2 The Risk Challenge
3.3 Risk Management and Residual Risk
3.4 Mitigation through Controls
3.5 Risk Registers and Appetites
3.6 The Risk Policy
3.7 Enterprise-wide Risk Management
3.8 Control Self-assessment
3.9 Embedded Risk Management
3.10 The Internal Audit Role in Risk Management
3.11 New Developments
Summary and Conclusions
Assignments and Multi-choice Questions

Internal auditors have derived key messages about the internal audit product based on the growing demand for suitable risk management in all organizations. In an interview with *Internal Auditing* magazine, David Brilliant has expressed this change and has built on the auditors' third paradigm:

> The fear was expressed that too many internal auditors are focused on what is happening inside their business and are not up to speed with the complexity of the external business and commercial environment. Failing to understand the external environment meant that internal auditors would struggle with the process of identifying risks.

Brilliant categorized these risks under the following headings:

- understanding the business products
- knowing the market place and custom
- examining the business risk process
- people behaviour
- management quality
- the changing environment.

> . . . It has to be remembered that organisations change just as people do. The process of change also can create risks as well as opportunities. So internal auditors should think risk and survive.[2]

Many view the new challenges from risk management as raising the bar for the internal auditor. This has been described in the *Internal Auditor* magazine:

> 'This movement away from compliance toward proactive involvement in risk management and governance will necessarily change the emphasis of audit shops and increase awareness of the types of activities they should engage in,' says Larry Rittenberg . . . 'the change in focus may represent a challenge for some, but for many the new standards will simply reflect the leading edge activities they already practice' . . . By mandating involvement in risk management and governance processes, the rewritten standards elevate the internal audit activity to a more strategic level within the organization . . . The revised standards name consulting services along with assurance as a key *raison d'être* for internal auditing, making it clear that aiding management should be a significant part of internal auditing's focus.[3]

3.1 What Is Risk?

We need go no further than the work of Peter L. Bernstein to get an insight into the quality of risk:

> The word 'risk' derives from the early Italian risicare, which means 'to dare'. In this sense, risk is a choice rather than a fate. The actions we dare to take, which depend on how free we are to make choices, are what the story of risk is all about. And that story helps define what it means to be a human being.[4]

This immediately introduces the concept of choice when it comes to risk – not simply being subject to risks as a part of life, but being in charge of one's destiny as there is much that we can control if we have the time and inclination to do so. The stewardship concept underpinning corporate governance forces management to seek out risks to the business and address them, where appropriate. Peter L. Bernstein goes on to suggest: 'The capacity to manage risk, and with it the appetite to take risk and make forward-looking choices, are the key elements of energy that drives the economic systems forward.'[5]

For those who are not convinced, we can turn to an article on risk taking that includes an interesting point:

> The best-paid man in Britain was revealed yesterday as a 52 year old investment manager who works from a small nondescript office. He earned an estimated £50 million last year for taking high risk bets predicting the movement of the interest rates and the path of the US dollar and Japanese yen on behalf of well heeled investors.[6]

The point is that success in business and the public sector is intimately tied into the act of risk taking. Risk arises from uncertainty and controls are based on reducing this uncertainty where both possible and necessary. HM Treasury defines risk as 'the uncertainty of outcome within a range of exposures arising from a combination of the impact and probability of potential events'. While the IIA Glossary defines risk as 'the uncertainty of an event occurring that could have an impact on the achievement of objectives. Risk is measured in terms of consequences and likelihood.'

Throughout this chapter, we will develop a model to consider risk and risk management. The first part of our first model appears as shown in Figure 3.1.

There are risks out there and they impact on our existence. Many of these risks arise in totally unexpected ways and can have a major effect on the key aspects of our lives as shown in this simple example: 'Scientist Barry Mathews went to the North Pole and back without mishap. But

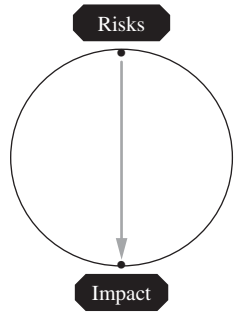


FIGURE 3.1 Risk management (1).

when it came to getting his photographs developed, the expedition ended in disaster. The store lost all the pictures the climate expert took on his Arctic journey – and Dr Mathews is now suing for £30,000, the cost of a return trip.'[7]

Most people have a vague awareness of the risks that exist in the wide world. Many associate risk with known benefits and perhaps view this as the price of these benefits. When the motor car was first invented, it was seen as a major breakthrough in transportation and apart from the high costs of the earlier vehicles, there were very few drawbacks as the next quotation illustrates: 'I hope this sort of thing will never happen again. Coroner at the inquest 100 years ago yesterday into the death of pedestrian, Bridget Driscoll, of Croydon, in the first recorded fatality involving a motor car.'[8]

3.2 The Risk Challenge

We now move into the field of seeing risk as a dynamic force that can be understood, considered and then acted on. Before we get there, it is as well to note a few more examples of what happens when serious risks run out of control:

> The search goes on into who should take responsibility for the boiler explosion which wrecked a tower block. The blast at Kerrin Point on the Ethelred Estate, Kennington, on June 26 left 11 people injured and more than 100 homeless. Now a report by consulting engineers Ove Arup has highlighted a catalogue of errors, and a probe has been launched by Lambeth Council . . . Tory councillor David Green said, 'I am appalled to learn that a Lambeth worker actually signed the boiler off as safe, this person must be identified and, if necessary, disciplined.'[9]

> Two senior hospital managers kept their jobs despite losing £500,000 to a fraudster. The decision has been slammed by union bosses who claim their members would have been sacked. The loss at St. Thomas' Hospital Waterloo was eventually whittled down to £376,670 – enough to run an NHS ward for a year.[10]

> Families of victims of the human form of mad cow disease claimed yesterday that an inquiry into the crisis will allow those responsible to 'get away with murder'. Lord Justice Phillips upset them by insisting that the purpose of his investigation was not to attribute blame. The primary objective was 'to identify what went wrong and why, and to see what lessons can be learnt'. He told a preliminary session before the public inquiry starts in March. The judge also revealed that civil servants who could be found at fault have been guaranteed immunity against disciplinary action. His words brought protests from some among more than 20 families who have lost children to the CJD disease, the human form of BSE.[11]

> Thousands of patients' lives are being put at risk because many operations are carried out by unsupervised trainee doctors, a report revealed. The study found that one in five operations carried out between 6pm and midnight were performed by trainee doctors. Almost half the operations involved trainee anaesthetists.[12]

The popular press is full of stories where things have gone terribly wrong. It seems that the mere act of walking out one's door, or getting into a car, or jumping into a swimming pool can mean disaster, injury or even death. We have said that controls are ways of minimizing risk and uncertainty and turning once again to Bernstein, we can obtain a perspective of this concept of control: 'But if men and women were not at the mercy of impersonal deities and random chance, they could no longer remain passive in the face of an unknown future. They had no choice but to begin making decisions over a far wider range of circumstances and over far longer periods of time than ever before.'[13]

We now arrive at the view that risk represents a series of challenges that need to be met. Also, the key feature of this challenge is that it appears when a major decision has to be made. Risk has no real form unless we relate it to our own direction, which is what we are trying to achieve. It is the risks to achieving objectives that affect us, in that they detract from the focus on success and stop us getting to the intended result. We may add to the risk model and may incorporate this feature into the existing dimensions in Figure 3.2.

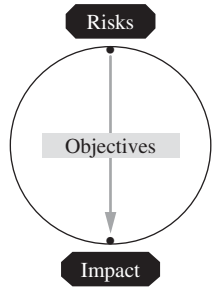


FIGURE 3.2 Risk management (2).

In this way, the impacts become the effect the risks have on the objectives in hand. Good systems of risk management keep the business objectives firmly in mind when thinking about risk. Poor systems hide the objectives outside the model or as something that is considered peripheral to the task of assessing the impact of the risks. In reality. it is not as simple as this. The act of setting objectives in itself is based on real and perceived risks, that is, some uncertainty about the future. Eileen Shapiro brought home this point in her book *Fad Surfing in the Boardroom*:

> Most organisations create a vision but they cannot create one based on a 20/20 understanding of the future as this is impossible. Better to create the vision in steps, as the future changes one adapts and flexes and so capitalise on opportunities as they arise and respond to threats. Mission statements then communicate the vision of itself and its future. In the perfect world of plans, a blueprint can be laid out, with timetables and responsibilities. In the messy world of bets, circumstances shift unexpectedly and odds change – not an environment in which inviolable plans and rigid schedules will necessarily be helpful.[14]

In recognition of this, we can adjust slightly our risk model to make the risk component interactive – in that the objectives are themselves set by reference to the uncertainty inherent in organizational climate in Figure 3.3.

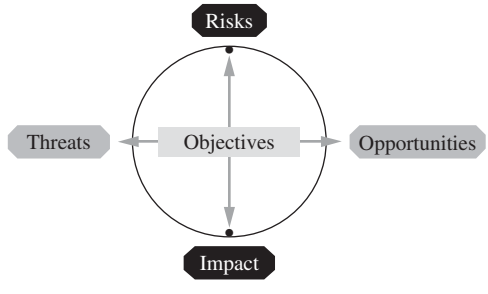


FIGURE 3.3 Risk management (3).

The other concept that needs to be considered is that risk, in the context of achieving objectives, has both an upside and a downside. In our model, we call these threats and opportunities. That is, it can relate to forces that have a negative impact on objectives, in that they pose a threat. Upside risk, on the other hand, represents opportunities that are attainable but may be missed or ignored, and so mean we do not exceed expectations. This is why risk management is not really about building bunkers around the team to protect them from the outside world. It is more about moving outside the familiar areas and knowing when and where to take risks. This is quite important in that if we view controls as means of reducing risk, we can now also view them as obstacles to grasping opportunities. So risk management is partly about getting in improved controls where needed and getting rid of excessive controls where they slow proceedings down too much. In other words, making sure controls are focused, worth it and make sense. We can turn once more to Peter Bernstein for a view of where opportunity fits into the equation: 'all of them (past writers) have transformed the perception of risk from chance of loss into opportunity for gain, from FATE and ORIGINAL DESIGN to sophisticated, probability-based forecasts of the future, and from helplessness to choice.'[15]

The original King report (see Chapter 2) also acknowledges the two sides of risk by suggesting: 'risk should not only be viewed from a negative perspective. The review process may identify areas of opportunity, such as where effective risk management can be turned to competitive advantage.' The next point to address is the basic two dimensions of measuring risk. That is, as well as defining the impact of the risk, we also need to think about the extent to which the risk is likely to materialize. To incorporate this feature into our risk model, we need to add a separate box that provides a grid of likelihood and impacts considerations regarding the effect of the risk on the set objectives in Figure 3.4.

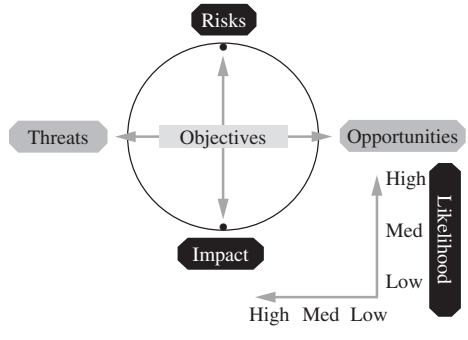


FIGURE 3.4 Risk management (4).

Having established the two aspects of risk, we can start to think about which risks are not only material, in that they result not only in big hits against us, but also whether they are just around the corner or kept at bay. Since risk is based on uncertainty, it is also based on perceptions of this uncertainty and whether we have enough information on hand. Where the uncertainty is caused by a lack of information, then the question turns to whether it is worth securing more information or examining the reliability of the existing information. Uncertainty based on a lack of information that is in fact readily available points to failings in the person most responsible for dealing with the uncertainty. There is much that we can control, if we have time to think about it and the capacity to digest the consequences.

3.3 Risk Management and Residual Risk

Risk management is a dynamic process for taking all reasonable steps to find out and deal with risks that impact on our objectives. It is the response to risk and decisions made in respect of available choices (in conjunction with available resources) that is important and the IIA has made the pertinent point that: 'Although organisations use the term risk management frequently (and it is used here for lack of better terminology), it too is misleading, because risk is never actually managed. It is the organisation that is managed in anticipation of the uncertainty (and opportunities) presented by risk in the environment.'[16]

So organizational resources and processes are aligned to handle risk wherever it has been identified. We are close to preparing the risk-management cycle and incorporating this into our original risk model. Before we get there, we can turn to project management standards for guidance on the benefits of systematic risk management which include:

- more realistic business and project planning
- actions implemented in time to be effective
- greater certainty of achieving business goals and project objectives
- appreciation of, and readiness to exploit, all beneficial opportunities
- improved loss control
- improved control of project and business costs
- increased flexibility as a result of understanding all options and associated risks
- fewer costly surprises through effective and transparent contingency planning.[17]

But remember, some risks are so unusual that they are hard to anticipate, as another example illustrates:

> The stewardesses were used to dealing with the odd first-time flier suffering from anxiety. But this was something no amount of training could have prepared them for. As BA 837 reached its cruising height of 33,000 ft en route from Birmingham to Milan, the co-pilot began getting the jitters. Looking out through the cockpit window to the ground six miles below, he confessed to his astonished fellow crew members that he was afraid of heights. Initial attempts to calm him down failed and the plane – operated by Maersk Air on behalf of British Airways – was forced to divert to Lyon so he could get medical treatment.[18]

Before we can delve into risk management, we need to make a further point, that is, that risk management is mainly dependent on establishing the risk owner, or the person most responsible for taking action in response to a defined risk, or type of risk, or risk that affects a particular process or project. The Turnbull report (see Chapter 2) on corporate governance for listed companies contains the following provisions regarding risk management:

> The reports from management to the board should, in relation to the areas covered by them, provide a balanced assessment of the significant risks and the effectiveness of the system of internal control in managing those risks. Any significant control failings or weaknesses identified should be discussed in the reports, including the impact that they have had, could have had, or may have, on the company and the actions being taken to rectify them. It is essential that there be openness of communication by management with the board on matters relating to risk and control. (para. 30)

When reviewing reports during the year, the board should:

- consider what are the significant risks and assess how they have been identified, evaluated and managed;
- assess the effectiveness of the related system of internal control in managing the significant risks, having regard, in particular, to any significant failings or weaknesses in internal control that have been reported;
- consider whether necessary actions are being taken promptly to remedy any significant failings or weaknesses; and
- consider whether the findings indicate a need for more extensive monitoring of the system of internal control. (para. 31)

The government position is found in the HM Treasury guidance on strategic risk management which says: 'The embedding of risk management is in turn critical to its success; it should become an intrinsic part of the way the organisation works, at the core of the management approach; not something separated from the day to day activities.' (para. 9.1)

To summarize the risk-management process, we can turn again to the risk model in Figure 3.5.

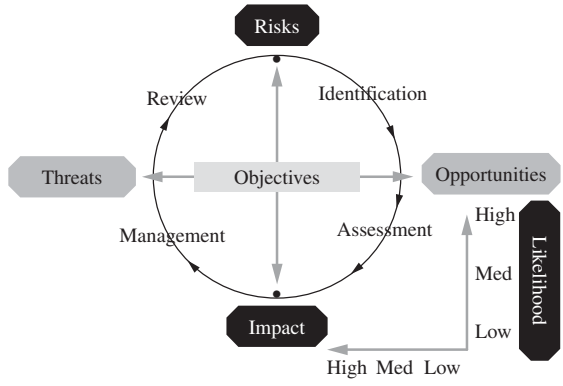


FIGURE 3.5 Risk management (5).

The stages of risk management are commonly known as:

Identification The risk-management process starts with a method for identifying all risks that face an organization. This should involve all parties who have expertise, responsibility and influence over the area affected by the risks in question. All imaginable risks should be identified and recorded. In 1999, Deloitte and Touche carried out a survey of significant risks in the private sector with each risk scored from 1 (low level of concern) to 9 (high level of concern) with the following summary results:

	Score
Failure to manage major projects	7.05
Failure of strategy	6.67
Failure to innovate	6.32
Poor reputation/brand management	6.30
Lack of employee motivation/poor performance	6.00[19]

Business risk is really about these types of issues, and not just the more well-known disasters, acts of God or risks to personal safety.

Assessment The next stage is to assess the significance of the risks that have been identified. This should revolve around the two-dimensional impact, likelihood considerations that we have already described.

Management Armed with the knowledge of what risks are significant and which are less so, the process requires the development of strategies for managing high-impact, high-likelihood risks. This ensures that all key risks are tackled and that resources are channelled into areas of most concern, which have been identified through a structured methodology.

Review The entire risk-management process and outputs should be reviewed and revisited on a continual basis. This should involve updating the risk-management strategy and reviewing the validity of the process that is being applied across the organization.

The above cycle is simple and logical and means clear decisions can be made on the types of controls that should be in place and how risk may be kept to an acceptable level, notwithstanding the uncertainty inherent in the nature of external and internal risks to the organization. In practice, the application of this basic cycle does cause many difficulties. Most arise because we impose a logical formula on an organization of people, structures and systems that can be complicated, unpredictable, vaguely defined and perceived, emotive and in a state of constant change. Most risk-management systems fail because the process is implemented by going through the above stages with no regard to the reality of organizational life. Managers tick the box that states the stages have been gone through and eventually the board receives reports back that state risk management has been done in all parts of the organization. Our risk models will have to be further developed to take on board the many intricacies that have to be tackled to get a robust and integrated system of risk management properly in place. The real-life problems have been alluded to by Tim Crowley in his comments on risk management in the National Health Service:

> A comprehensive system of controls assurance in the NHS – covering financial, organisational and clinical risk – moved a step closer this week as new guidance and control standards were unveiled in London . . . Eighteen standards on risk management and organisational controls, covering areas such as health and safety, infection control, waste management and catering, have been issued. Health bodies will have to self-assess their performance against these standards using a prescribed scoring system and drawing up corrective plans. But Tim Crowley, head of internal audit at Mersey Internal Audit Agency said, 'The standards should be seen as a starting point. The problem with issuing standards is that you can get a minimalist response. Health authorities and trusts should identify their own unique set of risks in terms of their own agenda and risk profile . . . ' the controls assurance initiative is seen as a major opportunity for internal auditors, giving them a wider remit to vet areas outside the financial arena. The enhanced code is in line with the recommendations of the recent Turnbull committee report on internal control issues in the private sector.[20]

The IIA has sponsored work by PwC through the IIA Research Foundation in 2000, which was published as a booklet entitled *Corporate Governance and the Board: What Works Best* (pp. 12–13). This has made clear the importance of risk management to the board and confirmed that organizations should have in place: 'an effective, ongoing process for identifying risk, measure its impact against a varied set of assumptions and do what's necessary to proactively manage it'. They go on to argue that:

> Second, the board also must be certain it is apprised of the most significant risks, and determine for each whether the right actions are being taken . . . A director of one company laments,

> 'Our board isn't dealing with risk in a systematic, broad manner and isn't addressing the entire universe of risk associated with strategy, culture, and people.' . . . Rather, it should be integrated within the way management runs the business, enriching that process and making it risk-focused. When done well, an enterprise-wide risk management architecture ensures risks are properly managed, assets secured, reputation protected and shareholder value enhanced.

3.4 Mitigation through Controls

We have suggested that risk management is an important part of the risk cycle, as it allows an organization to establish and review their internal controls, and report back to the shareholders that these controls are sound. The internal control framework consists of all those arrangements, and specific control routines and processes that drive an organization towards achieving objectives. In terms of risk management, we need to add to our risk model to set out the types of response to risk that ensure we can remain in control. Borrowing from the thinking of Peter Drucker, these responses consist of specific controls over processes and overall control over the delivery of the agreed strategy.

The way controls fit in with risk management is explained in the British standard on risk management:

> Those managing risk should prioritize changes to controls, taking into account the impact on other activities and the availability of resources. The control changes selected should be allocated to risk response owners and a schedule for their implementation should be prepared. Progress towards implementation of control changes should be monitored. The controls implemented should be documented.

Monitoring performance of controls

After control changes have been implemented and it becomes possible to gather data on the actual residual risk, the level of residual risk should be assessed. the same decision process should be used to decide whether to retain the residual risk or whether pursuing further control changes is worthwhile. The process should be repeated until the level of residual risk is within the risk appetite and pursuing further control changes does not seem worthwhile. The organization should monitor and test its controls to ensure:

- They have a named owner;
- They are defined, communicated and understood;
- Their implementation did not introduce any unacceptable additional risks;
- They are operating as designed, each is worthwhile, and collectively they managed the risk to an acceptable agreed level;
- They remain cost-effective; and
- That where deficiencies in the implementation or operation of controls are identified:
- The implications of control deficiencies not being remedied are established and options for resolution are identified;
- They are reported so that the consequence for the risk profile can be assessed; and
- The resolution of control deficiencies is planned and carried out.[21]

Our latest risk model becomes Figure 3.6.

We have developed 10 measures for addressing risks that have already been assessed for impact and likelihood, in the bottom left box of our model. Each of the 10 responses (5Ts and

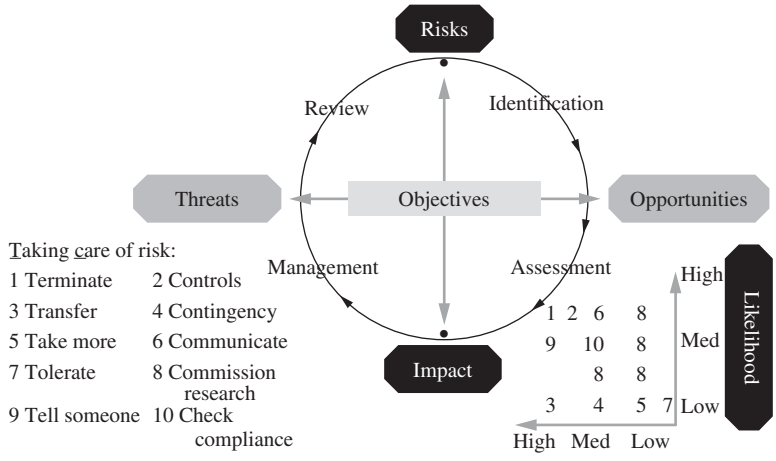


FIGURE 3.6 Risk management (6).

5Cs) are numbered and can be located within the appropriate part of the Impact Likelihood Grid in the bottom right of the risk model. For example, where we have assessed a risk as high impact but low likelihood, we may want to transfer (or spread) some of this risk, to an insurer as a suitable response (in this case number 3). The responses are further described:

1. Terminate Here, where the risk is great and either cannot be contained at all or the costs of such containment are prohibitive, we would have to consider whether the operation should continue. Sending sales reps to overseas countries may be common practice for enterprises that have a global growth strategy. Where certain locations are politically volatile, then we may have to take precautions in the way they conduct business in these countries and the type of security arrangements for high-risk sites. Where the costs of adequate security measures are not only sky high but also cannot give reasonable assurance that the sales people would not be attacked, kidnapped or simply caught up in dangerous situations, then we must decide whether to continue sending people to the country (or dangerous parts of the country) that is we may need to consider terminating the activity.

2. Controls One of the principal weapons for tackling risks is better controls. Note that this is the subject of the next chapter. Building on our example of overseas sales staff, after having assessed certain locations as high personal risk, we would go on to consider what measures we currently have in place and decide whether we are doing enough. Controls may cover local surveys, security personnel, formal guidance on socializing, say in the evenings, procedures for travelling and the use of drivers or guides, awareness seminars on ways of reducing the chances of becoming a target, good personal communications setup and so on. The degree of measures adopted may depend on the assessment of risk levels and changes in states of alert. The key question would be: Are we doing enough, bearing in mind what we know about this location?

3. Transfer Where the risks are assessed as high impact but low likelihood, we may wish to adopt a strategy of spreading risk, wherever possible. High-likelihood risk will be hard to transfer because all parties involved will want to be fully recompensed to the value of the impact of the risk. It is only where there is some uncertainty that transfers are more appropriate. Turning again to the running example, we may spread the impact of the risk by having an insurance policy that

covers overseas staff. Or we may employ an international firm or a local agency to perform the sales role in high-risk countries.

4. Contingencies A useful response to risk that is again high impact, low likelihood is based around making contingency arrangements in the event the risk materializes. The contingencies would focus on impacts that affect the continued running of the business, so that even after having installed preventive controls, there is still the chance that the risk may materialize. The overseas sales team may be covered by an evacuation procedure in the event that the risk of civil unrest materializes. This may involve access to a special charter plane that can be made available very quickly. The contingency plan may also cover business continuity for the sales lines that may be disrupted by the unrest. Many laypeople view risk management as essentially to do with contingency planning. That is, their rather narrow view of risk does not attach to the achievement of strategic business objectives and the need for processes to handle all material risks.

5. Take more One dimension of the risk-management strategy is derived from the upside risk viewpoint. Where the impact, likelihood rating shows operations located down at low/low for both factors, this does not necessarily mean all is well. Risk management is about knowing where to spend precious time and knowing where to spend precious resources. Low/low areas are ripe for further investment (for commercial concerns) or ripe for further innovative development (for public sector services). In the overseas sales example, we may wish to send out teams to countries that had a reputation for instability, but are slowly settling down and are open for business. Peter Bernstein has provided a view on this need to exploit opportunities to stay ahead of the game: 'The essence of risk management lies in maximising the areas where we have some control over the outcome while minimising the areas where we have absolutely no control over the outcome and the linkage between effect and cause is hidden from us.'[22]

6. Communicate One aspect of risk management that is often missed relates to high impact and either medium or high likelihood, where controls may not address the risk to an acceptable level, that is a strategy to communicate this risk to stakeholders and make them aware that this impairs the organization's ability to be sure of success (at all times). Communicating risk is a completely separate discipline and sensitive stock markets and high-profile public services have a difficult task in managing expectations, handling price-sensitive information and keeping politicians and the media happy. Some argue that the financial misstatement scandals in 2002 were fuelled by markets that demanded rapid and linear profit growth and resented bad news. Success in communicating risk is mainly based on a trust relationship between the giver and the receiver and the degree of consistency in the messages given. For our overseas sales people, we may simply publish the national statistic on trouble spots and rates of infectious diseases, and tell people about the known risks before they accept assignments. This is particularly helpful where there is little scope to establish robust controls in the area in question, where matters may be outside of our control.

7. Tolerate The low/low risks that come out of our assessment will pose no threat and as such can be tolerated. This stance may also relate to high-rated risks where we really have no option but to accept what is in front of us. At times where we install more controls over an area to increase the level of comfort, people adjust other controls so they fall back to what they see a comfortable position. Extra checking installed in one part of a system can lead to a slackening of checks in another as people make this adjustment. Going back to the work of Peter Bernstein, we can see this very point illustrated:

> Finally, the science of risk management sometimes creates new risks even as it brings old risks under control. Our faith in risk management encourages us to take risks we would not otherwise take. On most counts, that is beneficial, but we must be wary of adding to the amount of risk in the system. Research reveals that seatbelts encourage drivers to drive aggressively. Consequently, the number of accidents rises even though the seriousness of injury in any one accident declines.[23]

For our sales reps, this may mean the risks of communicable disease in part of the world that they travel to may be low impact (because the sales team have had all the jabs) and low likelihood (because the areas visited have good sanitation infrastructures). Any remaining risk may simply be tolerated.

8. Commission research We have argued that risk revolves around uncertainty as to the future. Gamblers are well versed in this and believe that they can beat the odds or simply enjoy placing bets because of non-financial reasons. Many risk-management systems are too rigid, in that they depend on quick assessments and a risk register that shows the agreed strategy for action. More developed systems will allow some thinking time, where one decision may be to go and find out more about the risk, its impact and whether it will probably materialize – that is to commission further research. For the overseas sales team, we may ask an international consultant to travel to a possible 'hot spot' and report back on the local conditions and risks therein. Or we may ask the experts since the Foreign and Commonwealth Office (FCO) in its published *Risk Management Framework 2002* states that the FCOs aim is to promote internationally the interests of the United Kingdom and to contribute to a strong world community, and the FCO also has a specific responsibility to help identify and manage risks to British citizens abroad.

9. Tell someone Some high/high risks create a blockage, in that they can only really be resolved by parties outside of those participating in the risk-management exercise. Many such exercises grind to a halt as the responsibility for managing the risk in question does not reside with the people who are designing the risk strategy. A better response is to set out the unguarded risk and work out a strategy for relaying this position to the party who can tackle it and also refer the result up through the line. At times, if outside parties do not realize that their inaction has stopped progress in another area, they have no reason to address the problem. Using our sales team example, we may argue that the sales drive is affected by unreliable communications between head office and an assessment of business risk may make this a key barrier to successfully getting orders placed and turned around. The management strategy may suggest that there is nothing that can be done as communications networks are run by the country in question. A better response is to relay this information to the board and note that there is a danger of missing strategic growth objectives if it is left unattended. The board may be able to lobby the government in question or support bids to international development agencies for projects that improve global communications. While these moves may not lead to improvements straight away, it may over time facilitate progress.

10. Check compliance The final weapon in the arsenal of risk responses is often overlooked. This is to focus on areas where controls are crucial to mitigating significant risks, and to ensure that they are actually working as intended. Controls that counter more than one material risk are particularly important. These controls may be reviewed and tested by internal auditors or a specialist compliance team at the behest of management. We can make a final visit to our sales team, for example, a key control over the team may be a regional co-ordinator who ensures smooth transport between countries and keeps everyone in touch with product developments.

It may be essential that the co-ordinator sticks to their terms of agreement and any shortfalls will lead to significant exposure. The risk-management response may be based on reliance on a key control that, so long as it works, means the risk is mitigated – the strategy then is to focus on the existing control and strengthen it where possible, and ensure it does what it is meant to do. In this case, review the regional co-ordinators and check they are discharging their responsibilities properly. The Chartered Institute of Public Finance and Accountancy (CIPFA) has prepared a guide called *Risk Management in the Public Services*, which contains some straightforward points to break down the mystery of risk management:

> There is no mystery about risk management but there is a lot of jargon! It is really about decision making and enabling the process of taking risk:
>
> - what is the risk here? (risk identification)
> - what can it do to the desired outcome? (risk evaluation – magnitude)
> - how likely is it to happen (risk evaluation – probability)
> - does the benefit outweigh the risk? (risk/benefit analysis)
> - can we do anything to reduce the risk? (risk reduction)
> - has anything happened to alter the risk (risk monitoring)
> - what plans can we put in place in the event that the risk happens? (contingency/service continuity planning)
> - what insurance can we buy to mitigate the risk or can we contract out this risk? (risk transfer)
> - what financial provisions should we hold for the primary or residual risk (risk funding).

The 5Ts and 5Cs model provides a wide range of techniques for developing a suitable risk-management strategy in the top left corner.

3.5 Risk Registers and Appetites

The basic risk model has to be made more dynamic to incorporate the next risk tool, which is the risk register in Figure 3.7.

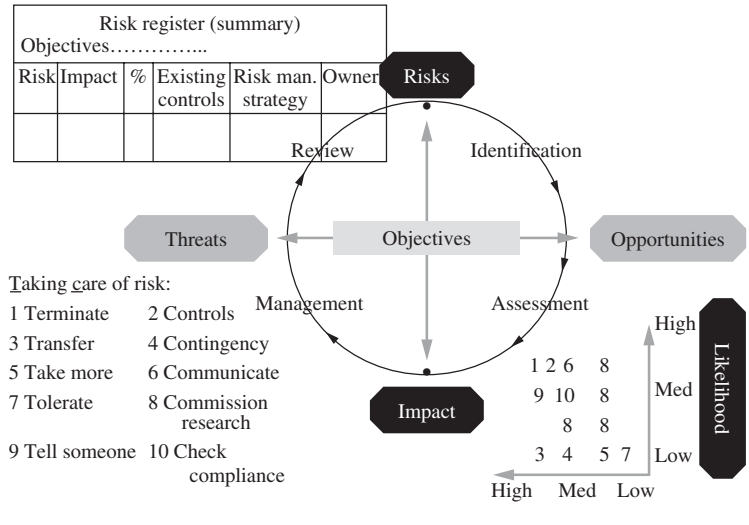


FIGURE 3.7 Risk management (7).

The subject of risk registers has a very interesting past. Project managers have used them for a long time as they assess risks at an early stage in a large project and enter the details in a formal record, which is inspected by the sponsors. The insurance industry again is well used for documenting assumptions about risk and using this to form judgements on where to offer insurance cover and what aspects of an operation are included in this cover. More recently, they have come to the fore as an important part of general business risk management. Risk registers act as a vehicle for capturing all the assessment and decisions made in respect of identified risks. Moreover, the registers may form part of the assurance process where they can be used as evidence of risk containment activity, which supports the statement of internal control (SIC). We have suggested that risk management is simply the task of defining risk, identifying risks, assessing this risk for impact and materiality and then devising suitable ways of dealing with more significant risks. Risk registers can be attached to this process to record the above stages and end up with both a record and an action plan. The register in our model in Figure 3.7 is a basic version that details the key objectives in question, the risks that have been identified by those closest to the action, their impact and likelihood and then a set of actions required to reflect the adopted strategy, which is then the responsibility of the risk owner. The register should be updated to reflect changes in the objectives, external and internal risks and controls, all of which in turn happens because of changes in the environment within which we operate. What goes in the register and what we document as significant as opposed to immaterial risk depend on the perception of risk, that is, the risk appetite, or what some call the risk tolerance. An elementary diagram forms the basis for a consideration of risk appetite in Figure 3.8.

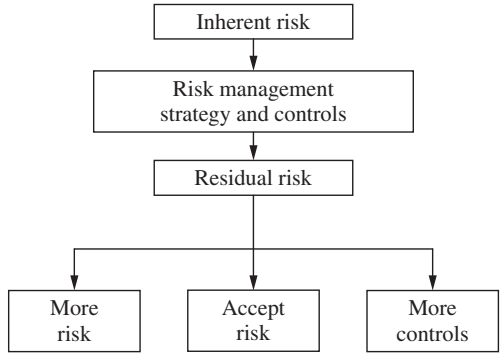


FIGURE 3.8 Risk appetites.

The risk appetite defines how we see residual risk, after we have dealt with it through an appropriate strategy, and whether it is acceptable or not, that is, is the risk acceptable as it stands or do we need to do more to contain it, or perhaps exploit areas where risk is too low? We need to turn once again to Peter Bernstein for an authoritative view on risk appetites. In short, it all depends: 'Few people feel the same about risk every day of their lives. As we grow older, wiser, richer, or poorer, our perception of risk and our aversion to taking risk will shift, sometimes in one direction, sometimes in the other.'[24]

The concept of risk appetite (or tolerance) is very tricky to get around. The contrasting positions are that the board sets a clear level of tolerance and tells everyone inside the organization; or that people are empowered to derive their own levels based around set accountabilities. These accountabilities mean defined people are responsible for getting things right and also must

explain where this has not happened and things are going wrong. HM Treasury (Strategic Risk Management) suggests that:

> Risk appetite is the amount of risk to which the organisation is prepared to be exposed before it judges action to be necessary . . . Risk appetite may be very specific in relation to a particular risk, or it may be more generic in the sense that the total risks which an organisation is prepared to accept at any one time will have a limit . . . Any particular organisation is unlikely to have s single risk appetite. The tolerable extent of risk will vary according to the perceived particular risks . . . The most significant issue is that it is unlikely, except for the most extreme risk, that any particular risk will need to be completely and absolutely obviated . . . Identification of risk appetite is a subjective . . . issue . . . (para. 6.1).

While authoritative writers have argued that: 'risk like beauty is in the eye of the beholder. Although many people associate risk with loss of assets, the concept is viewed by the auditor as much broader.'[25]

If an organization gets the risk tolerance wrong, then key stakeholders may well misunderstand the extent to which their investment is insecure, and conversely, where corporate risk tolerance is low, returns on investment may be likewise restrained. Funds will move in accordance with the level of risk that they are attracted to, so long as this level has been properly communicated to all interested parties as the following court case suggests:

> Merrill Lynch court battle with Unilever involved a £130 m claim from Unilever alleging that Merrill had pursued a too-high risk strategy was settled for around £75 m. During the trial a metaphor was used: Fund management and risk is like driving a car – If you can see the road, you drive faster; if it is foggy you slow down . . . One witness said: 'If you think you can see clearly, you should go faster . . . ' to which the judge said, 'The better the driver, the more justifiable it is for him to go at 90 rather than 70 mph?'[26]

Risk appetite varies between organizations, departments, section, teams and more importantly between individuals, and this appears in their behaviour:

> Stable lad Phil Sharp was hailed a hero last night after he refused to leave his mount Suny Bay during a bomb scare. While the rest of the course was being evacuated, he stayed with his horses in the stables. For two hours he tended eight-year-old Suny Bay and gave water to the other mounts until police ordered him to get out for his own safety.[27]

People go for jobs that suit their risk preference and a list of the most dangerous jobs around suggests that there are those that thrive on danger, and possibly achieve higher salaries than others:

Formula one driver	Bomb disposal officer
Test pilot	Member of the SAS
Circus entertainer	Film stuntman
Commercial driver	Oil rig worker
Scaffolder	Miner[28]

For each of the jobs listed above, the normalization equation means that the riskier the job the more detailed the controls over the task. Of all these jobs, it may be that the scaffolder has the less developed control arrangements and the net risk may make this job the most dangerous of all. If risk tolerance throughout an organization hovers at different levels with no rational explanation,

then we may well experience problems. Key performance indicators need to be set to take on board acceptable risk tolerances so that the organization is pulled in a clear direction and not subject to fits and starts as different parts of the organization slow things down while others are trying to speed them up. Where the entire organization has a high-risk tolerance, then it will tend not to install too many controls, particularly where these controls are expensive:

> Rail Chiefs refused to spend £5.2 million on modern safety measures which would have prevented the Paddington rail crash – in the year they paid out millions of pounds in dividends to shareholders, the public inquiry into the tragedy heard today . . . Railtrack admitted to the inquiry that it had neglected to investigate the cause of the regular incidents of Signals Passed At Danger. There were 37 in the Paddington area alone between August 1993 and July 1998.[29]

Returning to the IIA Research Foundation's *Corporate Governance and the Board* (p. 20), they confirm that risk appetite is a crucial concept for both the board and the CEO:

> One director's view – 'If the board isn't comfortable with the strategy that management has set, it should tell management to rethink it, and come back with something better. But, the board shouldn't be involved in developing strategy. That is, noses in fingers out' (page 1) . . . Although employees typically know what's going on before a crisis strikes, and 95 percent of CEOs say they have an open door policy and will reward employees who communicate bad news, half of all employees believe the bad news messenger runs a real risk of being seriously damaged . . . The 'tone at the top' establishes the true expectations for behavior. And the right behavior must be practice consistently by management – through good times and bad.

A lot of the 'true expectations for behaviour' revolve around perceptions of risk appetite. South Africa's King report develops this theme of risk tolerance:

> The board must decide the company's appetite or tolerance for risk – those risks it will take and those it will not take in the pursuit of its goals and objectives. The board has the responsibility to ensure that the company has implemented an effective ongoing process to identify risk to measure its potential impact against a broad set of assumptions, and then to activate what is necessary to proactively manage these risks. (para. 3.1.3)

The need for a clear message on risk acceptability appears again in the IIA.UK&Ireland's Professional Briefing Note Thirteen on Managing Risk states that: 'The assessment of risk and the determination of acceptable, or tolerable, levels of risk together with suitable control strategies are key management responsibilities.' (para. 5.1) The majority of risk-management guides refer to tolerance, acceptance, appetite and other such measures of what we have called unmanaged residual risk. The problem is that there is very little guidance on how to put this concept into action on the ground. Risk assessment is based on logic, measures and gut feeling. The gut feeling component is what makes it hard to set standards that, say, 10% level of risk is acceptable, or that a £100,000 is okay or that 1,000 errors per month will be tolerated. It is easier to say that major decisions shall not be made without having conducted a formal appraisal of risks and a determination of the optimal way of managing these risks. An even better stance would be to add that the context of risk assessment is based on transparency, integrity and accountability, which is good corporate governance. So keeping within these values while applying competence and robust approaches to measuring and managing risk takes us closer to a risk tolerance level, albeit somewhat implicit. The Institute of Risk Management (in conjunction with the National Forum

for Risk Management in the Public Sector (ALARM) and the Association of Insurance and Risk Managers (AIRMIC)) has prepared a risk management standard in 2002, which states that:

> When the risk analysis process has been completed, it is necessary to compare the estimated risks against risk criteria which the organisation has established. The risk criteria may include associated costs and benefits, legal requirements, socio-economic and environmental factors, concerns of stakeholders, etc. Risk evaluation therefore, is used to make decisions about the significance of risk to the organisation and whether each specific risk should be accepted or treated.

One model used to assess risk appetite uses the scale in Figure 3.9.

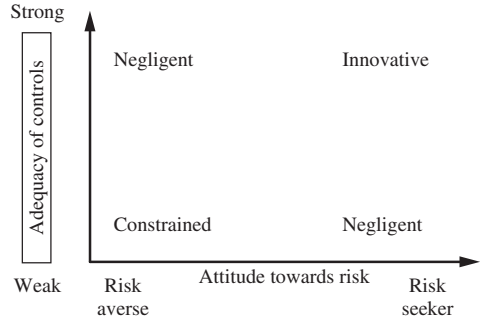


FIGURE 3.9 Risk attitudes and controls.

Here we balance the extent to which an organization's management seeks risk with the degree to which there are effective controls in place. Some people are active risk seekers as is clear from one article that describes how a gambling addict who ran up a £33,000 credit card bill has been jailed for a year and ordered to pay back the money. 'In his three month spending spree, he never won more than a fiver.'[30]

When considering risk tolerance, we need to build the control factor into the equation. Risk taking is fine so long as we can anticipate problems and work out how to counter them. Much confusion results from mixing gross and net risk. Risk, before we have put in measures to deal with it, is gross, or what we have called inherent risk. Risk that has been contained, so far as is practicable, is net, or what we have called residual risk. A high-risk occupation such as an astronaut may in practice be relatively safe because of the abundance of controls in place for each journey. The risk tolerance for space exploration agencies may be near on zero, with a focus on controls and quality assurance routines and numerous tests of these controls. Basil Orsini has considered diagnostic tools in risk management and among other things has argued that: 'the organization's approach to risk management reflects ethics and values as well as sensitivity to legal and political considerations.'[31]

Attitudes to risk tolerance become even more important when we consider the responsibilities of an organization to its stakeholders. The board members have a fiduciary duty to act in a reasonable manner and shareholders have a right to receive any announced dividends and to have their investment managed adequately. But, they will also need to understand the way the organization behaves towards risks. The Institute of Chartered Accountants in England and Wales (ICAEW) has commented on this very point:

> Enterprises in the same industry, facing similar risks, will often choose different risk management actions because different managements have different risk strategies, objectives and tolerances.

> It is therefore important that investors are made aware of the key business risks and how each risk is managed rather than given simply an assessment of the net risk.[32]

While companies need to work out their view on risk, it is much the same for government bodies. The National Audit Office (NAO) has reviewed risk management in government bodies along with the need to support innovation. They recognize that the civil service culture has: 'values, ethos, ethics and training underpinning the department's management approach – has traditionally been risk averse', and found that some 42% of departments regarded themselves as risk averse rather than risk taking. This may inhibit innovation in the way government services are designed, resourced and delivered. The NAO went on to document the now famous phrase that: *'the external auditor of government departments, the NAO, support well managed risk taking that is intended to result in tangible benefits for taxpayers'*. (para. 8)[33]

The NAO, in their *Focus* magazine of November 2000, go on to state that: 'Fear of audit is not a defensible excuse for not taking risks . . . auditors support risk taking as long as it is well managed'. The extent to which an organization fears risk, embraces risk or simply does not care whether a new strategy is risky may depend on whether there is a blame culture in place. Organizations with firm accountabilities but no blame culture may become risk seekers, and seek challenges as well as ways of managing the risks brought about by these challenges. Organizations that have more of a blame culture in place may well become extremely risk averse to avoid any potential finger pointing; or become extreme risk-takers but set up so that there is always someone to take the blame when systems/projects crash or scandals break out. Ironically these types of organizations may be seen as having strict standards with robust disciplinary machinery, but this is because of the high failure rate for new projects. As soon as a project falls over, someone is forced out of the organization. Accountability arrangements that are manipulated at one level in an organization to cover poor strategies or failures to implement or monitor strategy at a more senior level are a feature of blame-based organizational cultures. It is in this type of environment that it becomes hard to develop consistent messages about risk tolerance. The Turnbull report contains a reminder that board expectations must be made clear throughout the company. The section covering risk assessment includes questions that Turnbull states that each company should ask itself:

- Are the significant internal and external operational, financial, compliance and other risks identified and assessed on an ongoing basis? (Significant risks may, for example, include those related to market, credit, liquidity, technological, legal, health, safety and environmental, reputation and business probity issues.)
- Is there a clear understanding by management and others within the company of what risks are acceptable to the board?

A focused board with a well-considered strategy that is properly implemented, reviewed and further developed is the foundation for establishing risk tolerances that actually make sense to all managers and employees. Without these prerequisites there will always be problems where the concepts of accountability and blame become confused. One dynamic method of developing corporate risk appetites is to start with the board. If the board carry out a risk assessment to isolate their top ten risks then this reasoning may form the basis for categorizing risks throughout the organization which could then form the basis for developing risk registers at senior and middle level management. For each of the categories, top-down messages can be sent on what is acceptable and what may not be, depending on the type of operational risk and where it fits with the top ten board risks.

The British Standard on risk management has set out guidance on risk appetites and the risk profile that is mentioned below:

> Considering and setting a risk appetite enables an organization to increase its rewards by optimizing risk taking and accepting calculated risks within an appropriate level of authority. the organization's risk appetite should be established and/or approved by the Board (or equivalent) and effectively communicated throughout the organization. The organization should prepare a risk appetite statement, which may:
>
> - Provide direction and boundaries on the risk that can be accepted at various levels of the organization, how the risk and any associated reward is to be balanced, and the likely response;
> - Consider the context and the organization's understanding of value, cost effectiveness of management, rigour of controls and assurance process;
> - Recognize that the organization might be prepared to accept a higher than usual proportion of risk in one area if the overall balance of risk is acceptable;
> - Define the control, permissions and sanctions environment, including the delegation of authority in relation to approving the organization's **risk acceptance**, highlighting of escalation points, and identifying the escalation process for risk outside the acceptance criteria, capability or capacity;
> - Be reflected in the organization's risk management policy and reported upon as part of the organization's internal risk reporting system;
> - Include qualitative statements outlining specific risks the organization is or is not prepared to accept; and
> - Include quantitative statements, described as limits, thresholds or key risk indicators, which set out how certain risks and their rewards are to be judged and/or how the aggregate consequences of risks are to be assessed and monitored.
>
> The risk profile provides an overall picture of risk across an organization, within an organizational unit or for a defined area. The risk profile should convey the nature and level of risks the organization faces, the impact and likelihood of risk **incidents** on the organization and its stakeholders, and the effectiveness of controls in place to manage the risks. This may present an overview or a summary of the detailed risk documentation or show the full detail, whichever is most appropriate. Both the risk appetite and risk profile should be monitored by the Board (or equivalent) and formally reviewed as part of the organization's strategy and planning processes. This should consider whether the organization's risk appetite remains appropriate to deliver the organization's objectives in light of internal and external drivers and constraints.[34]

3.6 The Risk Policy

Our risk model has taken a clear form with many components that form the basis of effective risk management. In some organizations, risk assessment workshops are set up for key teams as a response to the trend towards CRSA programmes, often on the back of recommendations from the auditors or an external consultant. Teams get together, talk about risk and how it is being managed in their outfit and come out with a risk register that is filed and action points given to nominated managers. This annual exercise appears to be enough to satisfy the auditors and someone within the organization attempts to place the risk registers onto a database and eventually prepares summary reports for top management and the board. Better models use a key to highlight high impact, high likelihood (perhaps indicated in red), which then triggers a rapid response from the board who will want to know that action is being taken to handle key

exposures. The board then reports that it has reviewed the system of internal control, partly through the use of the risk-management process as described. This fairly typical arrangement has a number of shortcomings:

- Many staff do not know why they are engaged in the workshops and simply see it as a one-off exercise for the auditors.
- Many managers are reluctant to spend time on the workshops as they are busy doing 'real work'.
- Many workshops operate completely outside the important strategic realignment, restructuring and other change initiatives that are a feature of most large organizations.
- Many workshops are seen as clumsy devices for getting more work out of fewer staff.
- Many of the programme workshops result in masses of information that are impossible to co-ordinate or make into a whole.
- A lot of the action points that come out of the workshops are superseded by subsequent events and new developments.
- Most workshops are developed outside of the performance management system and there is little incentive to take on additional tasks that do not hit any key performance indicators (KPIs).
- Many see control self-assessment as relating only to the financial aspects of operations.
- Many workshop participants have already carried out risk assessment in their specialist fields of health and safety, security, project management, legal compliance and other areas of the business.
- Often the workshop facilitator introduces the event as a discrete exercise with no links to the organization's strategic direction.
- Many participants suffer the fallout from initiative overload and have spent much time in teambuilding events, performance review meetings, change programmes, budget reduction exercises, diversity training, e-business projects and so on.
- Many participants have experienced a culture where good ideas from staff never go anywhere and motivation levels are fairly low.

We could go on, where risk workshops or risk reviews based on survey or interviews are derived from an incomplete model of the risk-management system. As a result, we have developed our risk model to incorporate further dimensions that seek to counter the negatives listed above, as Figure 3.10 demonstrates. The amended model has built in three new factors (based around the risk policy), that is, the board sponsor, people buy-in and a chief risk officer (CRO). Each one is discussed briefly below:

Board Sponsor

Where there is no board member driving the risk-management process, it will tend to fail. The board makes a statement on the systems of internal control in the annual report and it is the board that reports that this system has been reviewed. The original King report (from South Africa) makes this point crystal clear:

> The board is responsible for the total process of risk management, as well as for forming its own opinion on the effectiveness of the process. Management is accountable to the board for designing, implementing and monitoring the process of risk management and integrating it into the day-to-day activities of the company. (para. 3.1.1) The board should set the risk strategy policies in liaison with the executive directors and senior management. These policies should be

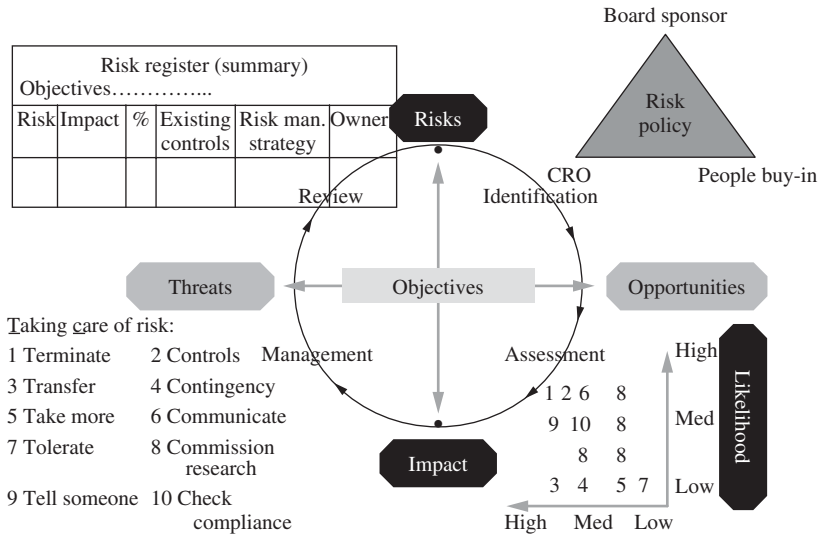


FIGURE 3.10 Risk management (8).

clearly communicated to all employees to ensure that the risk strategy is incorporated into the language and culture of the company. (para. 3.1.1)

In the government sector, this point is reinforced in HM Treasury's *Strategic Risk Management* guide which suggests key responsibilities for the accounting officer (AO):

> Reporting – The first mechanism to be implemented to assist with gaining assurance is a reporting system. This allows the management structure to report upwards about how risk management is being effected. This reporting system should be owned by, and report to, the AO through whatever mechanisms have been established for the co-ordination of risk ownership. (para. 8.1)

The Turnbull report contains guidance on the board's statement on internal control and states in paragraph 35 that:

> In its narrative statement of how the company has applied Code principle D.2 (reporting on internal controls), the board should, as a minimum, disclose that there is an ongoing process for identifying, evaluating and managing the significant risks faced by the company, that it has been in place for the year under review and up to the date of approval of the annual report and accounts, that it is regularly reviewed by the board and accords with the guidance in this document.

Turnbull represents aspirations that may not always be matched in practice. *Internal Audit and Business Risk* magazine details a report that warns about the difficulties in meeting these aspirations, where full risk reporting is not always achieved:

> Most companies only give brief and bland statements on their controls environment and risk frameworks. Just as the importance of good corporate governance is hitting the headlines after the Enron and Worldcom debacles, a recent survey has found that the majority of internal control reporting amounts to nothing more than 'mundane and nondescript waffle'. The report,

> Turnbull: An opportunity lost?, by Edinburgh-based business information researcher Company Reporting, says that because Turnbull encourages companies to discuss risk management processes and systems of internal control but stops short of requiring companies to disclose or discuss what the actual risks are, the majority of companies are providing mundane statements describing internal procedures that, without disclosure of the actual risks, lack context and relevance. The report says that 'as opposed to telling the analyst about risks and the systems or initiatives in place to address them, the majority of internal control disclosures appear designed to reassure analysts by bludgeoning them with extensive control system disclosure'. The report found that only 14% of companies have taken the initiative and gone beyond Turnbull to publish substantive risk disclosures that are complemented with the descriptions of the systems they have in place to address them.[34]

We are engaged in a continual search for better business practice. Meanwhile, the first cornerstone of the risk-management policy rightly sits at the board, as the highest part of the organization. The board may in turn establish a risk-management committee or look to the audit committee for advice and support, in respect of ensuring there is a reliable system for managing risks, or the audit committee may be more inclined to provide an independent oversight of the risk management and whether the arrangements are robust and focused. Regardless of the set up, the board remains responsible for ensuring management have implemented proper risk management. Some organizations have gone all the way and appointed a director of risk management, particularly in sectors such as banking, where the risk agenda is also driven by regulators. The board sponsor will direct the risk-management activity and ensure that it is happening and makes sense. One way of mobilizing the board and audit committee is to get them to participate in a facilitated risk assessment around the corporate strategy. Many risk consultants suggest that the board arrive at the top 10 or so risks to achieving the corporate strategy and make this information known to the management. The organization, particularly in the public sector, may also make this information available to outsiders as illustrated in material published by the Inland Revenue:

> Under the Modernising Government Action Plan all departments are required to make public the procedures they use for reaching decisions on risk for which they are responsible. We will quantify the risks to the Exchequer that have prompted the action being taken and we will set out what those risks are. Where there are other risks these will also be quantified where practicable and set out in impact assessment documents.

The board comes back into the frame when reviewing the risk-management process and ensuring it stands up to scrutiny. They would also consider the reports that come back from their management teams that isolate key risks and whether these are being contained adequately.

People Buy-In

Another problem with many risk-management systems is that they do not mean anything to the people below middle management level. They are seen as another management initiative that is 'done' to employees along with the multitude of other tools and techniques for improving performance and driving down costs. At worst, the employees are squeezed in between performance and costs in an attempt to work harder for less or the same recompense. In one risk-management policy, the organization had prepared a detailed diagram covering roles, responsibilities and relationships in the risk-management system with committees, boards, risk manager, facilitators, auditors and stakeholder analysis. At the bottom of the diagram is the

word 'individuals' with no further detail. The impression is that the risk-management process is something that happens to them. The individual is really the foundation of risk management, since it is what people do and how they behave that determines whether an organization succeeds or fails. It would have been more apt to start with the individual and work through how they fit into the risk-management process, or better still, how risk management can be made part of the way they work in future. This point has not been lost on the people who prepare guides to risk management and several extracts demonstrate the significance of 'people buy-in' for successful risk management. Basil Orsini has considered the people factor along with other factors in developing a risk-management diagnostic tool, and has developed five levels to assess the extent to which employees are encouraged and recognized for identifying risks and opportunities and for identifying risks that are not being managed:

> **Level 1:** A high level of skepticism exists within the organization. Staff perceives mixed messages on risk tolerances. Management does not value employee's contribution to risk management.
>
> **Level 2:** Management consults staff and allows them to participate in risk-management initiatives. Staff's contribution to managing risk is recognized on an ad hoc basis. Risk management is considered in rewards and sanctions.
>
> **Level 3:** The working environment supports a proactive approach to managing risks. Risk information is shared. A strong sense of teamwork exists across the organization.
>
> **Level 4:** Recognition and reward systems encourage staff to manage risks and to take advantage of opportunities. Management is committed to learning from positive and negative outcomes.
>
> **Level 5:** Management encourages employees to identify new challenges and opportunities, as well as risks that are not appropriately managed.[35]

The Institute of Risk Management's standard on risk management suggests that the focus of good risk management is the manager and employee responsible for the identification and treatment of these risks. The result of people buy-in is that we can get closer to a risk managed culture where people around the organization take responsibility for isolating risks and making sure they provide criteria for making key decisions. Gordon Hill has described the components of this risk managed culture as an environment that:

- enables people to take more effective decisions
- allows risks to be fully understood so that calculated risks can be taken
- encourages staff to consider the consequences of decisions and actions they take.[36]

A good starting place is to hold risk awareness seminars with managements, work teams and project team members. The idea is to tell people about the organization's risk policy and adopted approach to getting risk management accepted and implemented in the organization. Some organizations fail to inspire their employees because they have not bothered to tell them about the risk policy, the board's view on risk, including their own risk assessment and top 10 risks, and they do not explain how risk management can help them in their work. There is a useful model that can be applied to promoting successful seminars, by building several considerations

into the planning phase of the communications project (via the seminars). The models appear as follows:

Aims	*Have to*	*Should do*	*Want to*
1. Understand nature of risk	✓	✓	✓
2. Appreciate our risk policy	✓	✓	✓
3. Accept the need for control self-assessment	✓	✓	✓
4. Appreciate links to corporate governance	✓	✓	✓
5. Look forward to the risk workshops	✓	✓	✓

Along the top, we have three criteria, have to, should do and want to, as a way of measuring the success of the seminars. We want staff to understand that they have to attend the seminar (have to) and that they should really do so in furtherance of their responsibilities at work (should do). The final aspect to ensure success is that they would really enjoy the event (want to) and that the word spreads that it is fun and inspiring. Along the left we set the aims of the seminar. That is to get the entire concept of risk, risk policies and self-assessment onto the personal agenda of everyone. The awareness seminar will be designed to suit the needs of the organization and one version that suits small groups of say 10–16 appears below:

1. Pre-event work – send material to participants on risk policy and ask them to complete a self-assessment form on their understanding of corporate governance and risk management (the material may be posted on the intranet).
2. Introduction – key note from board sponsor on importance of risk management.
3. Introductions – from participants saying who they are, where they work and what they know about corporate governance and risk management.
4. Define risk – have some fun with a simple exercise of the risk of, say, coming to the seminar without reading through the advance material.
5. Exercise – list the benefits of good risk management (in pairs). Record their answers.
6. Introduce corporate governance in outline and explain the need to report on internal controls. The three components of integrity, accountability and openness can be used as a useful format.
7. Describe the components of the risk policy and how this should drive performance and accountability.
8. Explain the adopted control model, e.g. Committee of Sponsoring Organizations of the Treadway Commission (COSO) and get them to assess the control environment where they work.
9. Do an exercise on what makes for a good control. Draw out points relating to flexibility, ownership, risk focused, reasonable, cost efficient, simple, not excessive, accepted and understood, complied with and so on.
10. Explain how risk workshops (or other approaches such as questionnaires, reviews, interviews) will be used to implement risk assessment and risk management and introduce the risk cycle.
11. Describe the risk register and explain the links into corporate accountability and assurance reporting.
12. Main exercise (should last less than an hour) – get them into three subgroups to do a risk assessment of hosting a dinner party (you are new to the area), buying a family car (the group is the family) and planning a group holiday. They should agree the objective, brainstorm risks

at random, assess them for impact (where no controls exist) and likelihood with votes that they use to plot the numbered risks on the impact/likelihood grid.

13. Get all three groups back together and go through how they organized agreeing objectives, facilitating the event, isolating risks, rating them and locating them on the grid in terms of significance and likelihood.
14. Prepare a risk register for each exercise (dinner, car and holiday), and working on significant risks, set out existing or usual arrangements (controls), new activities required and how we assign ownership and develop action plans. Keep it simple and make it a fun event.
15. Review how the exercise enables us to get to key risks and develop consensus in designing a risk-management strategy and associated system of controls to both promote success and account for risks inherent in each activity.
16. Summarize and explain next steps and ask the key note speaker to describe the risk management and assurance reporting process.
17. Ask for feedback – use this to redesign the seminar.
18. Formally close the seminar and provide ongoing support through on-line material and discussion groups, and suggested links to useful websites.

Public Risk

In terms of risks affecting the public (in contrast to business risk), we will start to see young recruits with a good understanding of personal risks as this is now taught in school. The Department for Education and Skills has issued a statement on the management of risks affecting the public along with:

> a framework for Personal, Social and Health and Education and Citizenship across all four key stages from ages 5 to 16. It aims to help pupils develop the knowledge, skills and understanding they need to live confident, healthy, independent lives both as individuals and as members of society. Young people must be able to recognise the way in which their behaviour affects others, recognise their duties and responsibilities as well as rights, and receive support for their moral and social development. The framework includes the teaching or risk awareness within the curriculum as follows:
>
> - At key stage 1 – pupils should be taught rules for, and ways of, keeping safe, including basic road safety, and about people who can help them stay safe.
> - At key stage 2 – pupils should be taught to recognise the different risks in different situations and then decide how to behave responsibly, including sensible road use. Pupils should be taught about school rules on health and safety, basic emergency aid procedures and where to get help.
> - At key stage 3 – pupils should be taught to recognise and manage risk and make safer choices about healthy lifestyles, different environments and travel.[37]

In future, new recruits will arrive at an organization with the key question 'how do you manage risk here?' and feel quite comfortable working with whatever process has been developed and employed. Conversely, they will feel uncomfortable if there is no formal methodology in place. Returning to the present, the employer needs to convince staff that risk management can be applied to the business and drive the way we work towards achieving strategic and operational goals. Buy-in from a non-specialist employee makes everything else much easier, and means that corporate risk has value to front line staff. If staff buy-in is managed well, an organization may be able to unlock the potential, as described by Nancy Hala:

> Whose job is risk management? The short answer is: Everyone in the business. Because each individual in the company takes part in the organization's business activities, each individual takes risks. Whether or not these risks are actually addressed, however, depends on each employee's familiarity with the potential exposures associated with his or her job and the resources available to mitigate those exposures. Effective knowledge-sharing allows every one of the organization's employees, from staff level to leadership, to engage in risk management by organizing, categorizing, and monitoring risks as they relate to each business process. Knowledge-sharing across functions also enables employees to develop a big-picture view of the company and identify the enterprisewide risks that span the organization, as well as the interrelationships of those risks.[38]

If buy-in works for risk management, then the spin-off is that people build their own controls. CIPFA in their *Introduction to Risk Management in Central Government* (December 1999) supports the view that the most effective risk-management systems are fully integrated within the operations of an organization and go on to say that: 'in assessing risk management systems, it is essential to understand that controls are only as effective as the people within the organisation who operate the controls.'

Getting the message across is fundamental to good risk management and all means available should be used. Meanwhile, the Australian/New Zealand Risk Management Standards (AS/NZS 4360:1999) suggest that organizations need to communicate key risk messages through training and risk workshops, briefings, presentations, newsletters, websites, intranet, corporate plans and articles.

Chief Risk Officer

The second leg of the risk policy stool relates to the need for a person responsible for co-ordinating risk effort around the organization. This person proactively directs the effort and sets up systems that embed the risk policy into everyday activities. A version of a job advertisement for a business risk manager illustrates the importance of the new role:

> Reporting directly to the Audit Committee and Group Finance this role is a rare opportunity to join an exciting company and continue the development of the overall Risk Management framework for the business on a global basis. Skills include:
>
> - Sound knowledge of risk management techniques, corporate governance and audit assurance.
> - Highly developed communications and presentation skills.
> - The ability to ask the right questions and remain independent.
> - The ability to make the right practical decisions.
> - A dedicated, energetic and enthusiastic approach, and be a true team player.

Proponents of the role of CRO, such as Tim Leech, recognize the need for someone to pull the risk jigsaw together and make sense of it all for the board and senior management. They argue that we need to put right the silo reports on risks that are a feature of most big organizations. Still others, such as Terry Cunnington, have described arrangements where a risk assurance service provides enterprise risk management (ERM), internal audit and risk consultancy from one integrated team. Basil Orsini has explained how there needs to be a resource to provide expertise and direction on risk management by suggesting that there should be: 'Center(s) of excellence exist for risk management with the ability to advise on risk management issues on an integrated basis through multi-disciplinary teams.'[39]

Meanwhile the Audit Commission for Scotland's paper 'Shorten the Odds' (July 1999) describes the corporate risk manager and support services who support the council and its department in the effective development, implementation and review of the risk-management strategy and a corporate risk-management working group to share experience on risk, risk management and strategy implementation across the council.

A key role of the CRO would be to bring together bits of risk reporting. The problem of silo reporting on risk that we mentioned above is admirably described by Arthur Piper:

> Imagine for a moment that each reporting function within an organisation speaks a different language. Health and Safety officers speak German, risk managers French, internal auditors English, lawyers Spanish, treasury specialists Chinese, and insurance managers Japanese. All these different people then prepare and submit reports to the board of directors. If it is a typical UK board, you would not expect to find a polyglot among its members, therefore some form of interpretation would be needed to translate those different reports into a common language that the board could understand. At the moment, this analogy seems to fit perfectly well with the way that board receive assurances about the way risks are being identified, managed and controlled within their organisation.[40]

In developing the role of the CRO, great care must be taken. If this person becomes the risk manager, rather than risk co-ordinator, then there may be a perception that the postholder and no one else is responsible for managing risk. CIPFA has addressed this concern in their publication, *Risk Management in the Public Services*:

> In the public sector there are many cases where risk management is being practised under other names, such as health and safety, community safety, environmental management, emergency planning, treasury management and so on. But recognising this doesn't mean that they have to fall under the umbrella of some created function called risk management. What does need to happen is that every manager at every level needs to recognise risk management as part of their job – to explicitly consider the risks surrounding their everyday decisions.[41]

Nonetheless, there needs to be an in-house expert who can drive through the risk policy and make it work in practice. Their role may include:

- translating the board's vision on risk management;
- helping to develop and implement the corporate risk policy;
- ensuring the people buy-in mentioned earlier;
- providing training and awareness events where appropriate;
- helping respond to requirements from regulators that impact on risk-management systems;
- establishing a strategic approach to risk management across the organization with programmes, the appropriate approaches, tools and reporting arrangements;
- ensuring that the business is responding properly to changes and challenges that create new risks on a continuous basis;
- establishing a risk reporting system from managers in the organization that can be used to provide assurances that support the board review of internal control;
- helping facilitate risk-management exercises and programmes;
- becoming a centre of excellence on risk management and going on to develop an on-line support infrastructure, based on the latest technology that can be used by all parts of the organization.

- helping co-ordinate risk-management activities such as health and safety, security, insurance, product quality, environmental matters, disaster recovery, compliance teams and projects and procurement;
- providing advice on sensitive issues such as perceptions of risk tolerance and the consistency of messages in different parts of the organization;
- seeking to implement enterprise-wide risk management as an integrated part of existing processes such as decision making, accountability and performance management.

We could go on and there is a shortcut to defining the role of the CRO – it is to make good all aspects of our risk model and ensure that together they provide an effective system of risk management that is owned by all employees and integrated into the way the organization works. No risk policy will work without a commitment to resource the necessary process and ensure there is someone who can help managers translate board ideals into working practices. The IIA Research Foundation's booklet on *Corporate Governance and the Board: What Works Best* suggests that the CRO: 'acts as line managers' coach, helping them implement a risk-management architecture and work with it ongoing. As a member of the senior management team the CRO monitors the company's entire risk profile, ensuring major risks identified are reported upstream.' Each organization will develop a formula that suits and government bodies may well turn to the HM Treasury *Strategic Risk Management* guide for help as they argue that: 'The designated risk owners can be formed into a RM committee which reports to the Accounting Officer or acts as a subcommittee to the senior management board.'

Risk Policy

We have defined the main aspects that support the risk policy as board sponsorship, people buy-in and a source of expertise and assistance (the CRO). To close, it is possible to list the items that may appear in the published risk policy and strategy itself:

1. Define risk and state the overall mission in respect of risk management.
2. Define risk management and the difference between upside and downside risk.
3. Make clear the objectives of the risk policy – mention why we need a defined position on risk management.
4. Stakeholders and where they fit in – and the need to communicate a clear and reliable message.
5. Background to regulators and their requirements for risk management (and note on corporate governance code).
6. Position on appetite and whether the aim is risk avoidance, risk seeking or a measured balance.
7. Why bother? – list of benefits behind risk management; better controls and better performance and better accountability – impact on corporate reputation.
8. Background to the RM process (the risk cycle) and how it is integrated into decision making and planning, and performance management.
9. Risk responses and strategies leading to better certainty of achieving goals.
10. Internal controls – what this means with brief examples. The right control means putting in controls where risk is evident and getting rid of them where they are not required.
11. Training and seminars – importance and use.
12. Roles and responsibilities of all staff and specialist people such as board, CRO, internal audit, external audit and technical risk-based functions. Importance of the business unit manager.

13. Structures including board, audit committee, any risk committee and links to the CRO, quality teams and auditors.
14. Risk classifications or categories used in the risk-management process.
15. Tools and techniques – guidance on the intranet including a short guide to CRSA workshop (method, tools and principles involved).
16. Links to the overall internal control model that is applied with particular reference to the need for a good control environment to underpin the risk process.
17. Links to established risk assessment practices built into projects, security, contingency planning and so on.
18. Assurance reporting – giving overall responsibilities, review points, validation of reports and the use of risk registers – including regular updates.
19. Need for integration into existing management systems such as performance management.
20. Glossary of terms.
21. Where to go to for help.

The policy may be a brief document that gives an overview of the organization's position of risk management with clear messages from the board. The risk strategy will go into more detail and develop more guidance on how to put the policy into action. The British standard on risk management has described the importance of the risk-management policy:

The risk management policy should provide a clear and concise outline of the organization's requirements for risk management as an integral part of the organization's overall approach to governance. To achieve consistency of risk management activities across the organization, with appropriate variations in detail, the policy should contain a high level overview and description of the risk management process. The risk management policy should be:

- Owned by a manager, preferably at Board (or equivalent) level;
- Developed in consultation with key stakeholders;
- Developed with consideration of how the organization will monitor adherence to the policy and reference any relevant standards, regulations and policies that have to be included or taken into account; and
- Subject to quality assurance practices, e.g. document, change and version control.

Content of the risk management policy

The organization's risk management policy may include:

- **Governance**, outlining how risk management is governed;
- **Policy scope**, describing the purpose of the policy and who it is aimed at; describing the high level principles and the benefits of implementing risk management; setting out the objectives, including legal and regulatory requirements, and what it intends to achieve; and providing an explanation of the relationship with other policies;
- **Policy applicability**, setting out to whom and to what the policy applies;
- **Risk management process**, providing a high level overview and description of the risk management process adopted by the organization;
- **Risk appetite**, outlining the organization's risk appetite, thresholds and escalation procedure;
- **Reporting**, describing the purpose, frequency and scope of reporting;
- **Roles, accountabilities and responsibilities**, describing the high level roles, accountabilities and responsibilities in respect of risk management; and

- **Variations and dispensations**, stating whether variations or dispensations from the policy are allowed and, if they are allowed, describing the process for requests for this.[42]

3.7 Enterprise-wide Risk Management

Enterprise-wide risk management or ERM is simply the extension of risk management across the organization in an integrated fashion. This is in contrast to the old approach where specialist pockets of dedicated processes such as contingency planning were risk assessed but only at a local level for the process in question. Jim Deloach, Global Leader of Strategic and Enterprise Risk Consulting, Arthur Andersen, has said that:

> There is no one size fits all approach to ERM. That said, we do believe that any ERM project must begin with five essential actions:
>
> 1. establishing an oversight structure;
> 2. defining a common language and framework;
> 3. targeting risks and processes;
> 4. establishing goals, objectives, and a uniform process; and
> 5. assessing risk management capability.[43]

Before we delve into ERM further, there is a related point to clarify with the risk model we have been using throughout this chapter. The new risk model is amended in Figure 3.11. In the middle box, we have added **strategy** and **KPIs** to the original factor, **objectives**. We started with objectives as the driver for risk management and this viewpoint stands. What we are working towards is for risk management to be part of the strategic planning process and therefore integrated within the performance measurement system. This can be best illustrated with another model (Figure 3.12) that considers the role of risk assessment and where it fits into the organization's strategic analysis:

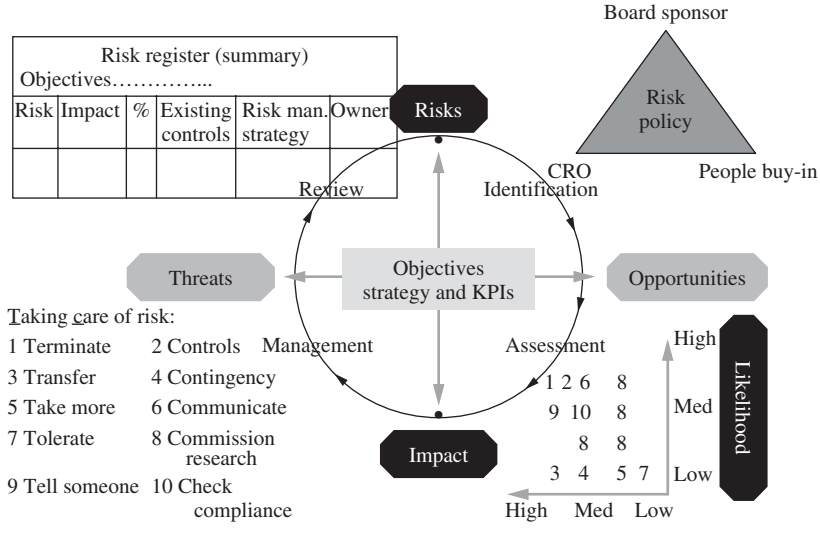


FIGURE 3.11 Risk management (9).

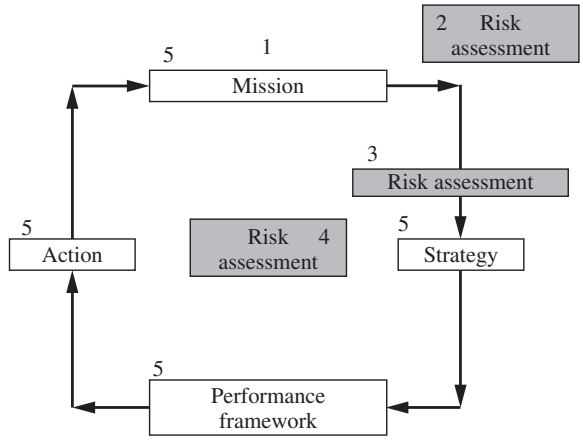


FIGURE 3.12 Stages of risk management.

The model is based on a simple management cycle with a mission that is translated into a strategy, which when implemented relates to performance measures that are used to monitor the progress of the adopted strategy and action taken to review and adjust. There are five development phases for risk assessment within the cycle as just described. Each of the five phases is noted as follows:

1. No risk assessment is carried out and the strategic management cycle takes no account of a formal identification and assessment of risk. There are very few organizations still at this stage. The policy may run along the following lines: 'many of our specialists people are already doing their own risk assessment anyway!'
2. Here risk assessment is an annual event that is a separate exercise, which is removed from the corporate strategy. It may be done once and then left, or carried out each year, mainly for the disclosure requirements where the organization reports that it has a risk-management system in place. Again, there is a minority of large organizations that take a mechanical view towards risk. The policy may run along the following lines: 'risk assessment is an annual exercise that is reported back to the board!'
3. Phase three places risk assessment inside the strategic management cycle so that as strategy is revisited during the year or whenever there is a major change in direction, the assessment of key risks is also addressed. Many organizations are at this phase, where risk assessment is a separate but component aspect of developing strategy. The policy may run along the following lines: 'risk assessment is built into our strategic analysis, and as strategy changes so do the risk management responses!'
4. This phase locates risk assessment right inside an organization's corporate heart. It drives the way objectives are set, the strategic framework, performance issues and monitoring and decision making. It involves a culture shift towards formally addressing risk as part of business life. Here, all key decisions, change programmes and underpinning projects and resource shifts derive from a consideration of upside and downside risks. Organizations that claim an ERM system is in place will have arrived at phase four. The policy may run along the following lines: 'risk assessment is at the core of our activities and drives setting objectives, strategy and performance reviews!'

5. The final phase drops the term 'risk' and it disappears altogether. Risk assessment is so immersed into the culture of an organization that it becomes an implicit part of the corporate and personal value system for everyone involved with the organization. There is no longer a need to talk about risk management and risk registers since it happens implicitly. The policy may run along the following lines: 'we no longer call it risk management, our values simply say that our people are taking good care of the business on behalf of our stakeholders!'

The key feature of the above model is that some organizations in high-risk businesses such as derivatives are already at phase five. But for corporate governance reporting purposes, they have to formalize their arrangements by designing a risk-management system, demonstrating that it works well and then slowly place it back into the infrastructure, like a ship's engine, quietly throbbing unseen in the background as it drives the ship forward.

The Government Experience

The task of spreading the risk message beyond a few specialist staff has not always been easy. While the private sector has been encouraged to develop risk-management systems to underpin their review of internal controls, the public sector has likewise been active in this field. The HM Treasury's *Strategic Risk Management* sets guidance for government bodies and has been adapted and adopted by the wide range of diverse organizations involved. Meanwhile, the Cabinet Office has reviewed the government's capability to handle risk and uncertainty and prepared a comprehensive report in August 2002 setting out the findings to date, including six key recommendations. Extracts from this report demonstrate the serious effort being made to get risk management installed across all parts of government:

> However, progress is uneven across government. There is plenty of good practice, but the coverage is not comprehensive. In particular, some of the application of risk management techniques has been mechanistic and not integrated into decision-making at the highest level. There is not always sufficient demand for good risk management (for example, from Ministers and senior officials) and the incentives could be strengthened (for example, by being linked to greater financial or management autonomy). Further, there is a perception amongst many senior officials that the Public Accounts Committee's high profile focus on policy and delivery failure (amplified by the media) inhibits innovation, despite the PAC emphasising its support for 'well judged risk taking'. (para. 23)
>
> Responsibility for handling risk should lie with those best placed to deal with it. This can only be judged on a case by case basis, but criteria include:
>
> - Competence – who has the skills and experience? And/or can best recruit and retain the right people?
> - Capacity – does the capacity exist? Can it be developed?
> - Public interest – is there sufficient assurance that the public interest will be protected?
> - Value for money – which will offer the best trade off between costs and benefits?
> - Management – can the arrangements be adequately managed?
> - Subsidiarity – operational decisions will often be best made by those closest to service delivery. (para. 45)

Most of the public sector have recognized the need to develop sound organization-wide systems of risk management.

Integrating Risks

In the past, risks were considered in isolation but ERM seeks to have risks considered across the entire organization along with a determination of how they fit together. The IIA Research Foundation booklet on *Corporate Governance and the Board: What Works Best* developed many themes that relate to ERM and documented one comment from a company director that 'Our board isn't dealing with risk in a systematic, broad manner and isn't addressing the entire universe of risk associated with strategy, culture, and people.' The report's authors argue that risk management should:

> be integrated within the way management runs the business, enriching that process and making it risk focused. When done well, an enterprise-wide risk management architecture ensures risks are properly managed, assets secured, reputation protected and shareholder value enhanced . . . the effective application (of RM) requires:
>
> 1. Line management embracing responsibility for risk.
> 2. Facilitation and support to assist line managers.
> 3. A culture that rewards the recognition, communication and management of risks.
> 4. Performance metrics to measure whether business units are taking the right risks to achieve the strategic objective.
> 5. Human resource performance assessment, compensation and incentive programs linked to manager's risk management performance.
>
> . . . the Board oversees all key risks and ensures a holistic, ongoing risk architecture to identify, manage and monitor risk – no matter what committee they set up to assist this task.

The Australian/New Zealand standards on risk management (AS/NZS 4360:1999) involve a six-step process:

1. support of senior management
2. develop the organizational policy
3. communicate the policy
4. manage risks at organizational level
5. manage risks at the program, project and team level
6. monitor and review.

While the King report makes it clear that: 'Risk management and internal control should be practiced throughout the company by all staff, and should be embedded in day-to-day activities', (para. 3.1.7) ERM makes risk management a board issue and sees the entire organization as the platform on which to assess and prioritize risk that together impact the entire strategy and reputation of the company. Christy Chapman has reported the 'big picture' on ERM in *Internal Auditor* magazine with the help of some of the consulting firms and there are interesting extracts from some of these viewpoints. KPMG suggests that: 'ERM is the lens that helps business leaders see how business opportunities can be tied to risk management in a way that creates value.' While PwC suggests that most boards and CEOs want three things from their ERM programmes:

- a proactive approach that focuses on more than just hazards;
- a truly holistic discussion of the various risks in terms of how the organization should operate and what board members and senior management should be concerned about, rather than a compendium of risk reports from all business units; and

- more robust ideas about how to better run their businesses.

the then consultants, Arthur Andersen, argue that:

> there is no one size fits all approach to ERM. That said, we do believe that any ERM project must begin with five essential actions:
>
> 1. establishing an oversight structure;
> 2. defining a common language and framework;
> 3. targeting risks and processes;
> 4. establishing goals, objectives, and a uniform process; and
> 5. assessing risk management capability.

While Deloitte & Touche separate the risk-management cycle into four stages:

1. identifying, assessing and prioritizing risks;
2. plans for assuring the effectiveness of the systems designed to protect the company and for further mitigating priority risks;
3. monitoring, reporting, governance issues and oversight; and
4. the organisation's sustainability, capability and continuous improvement.

Finally, Ernst and Young have identified six major components of effective risk management:

1. a risk strategy;
2. risk management processes;
3. appropriate culture and capability;
4. risk management functions;
5. enabling technologies; and
6. governance.[44]

This big picture really does use the entire organization as the canvas for risk management. In keeping with this analogy, we might suggest that the canvas is painted red, amber and green for high-, medium- and low-risk areas, which can be reviewed at board level as in Figure 3.13.

Each part of the organization will undertake risk assessment and compile risk registers containing the agreed risk-management strategy. Reports from each section will be aggregated to form a

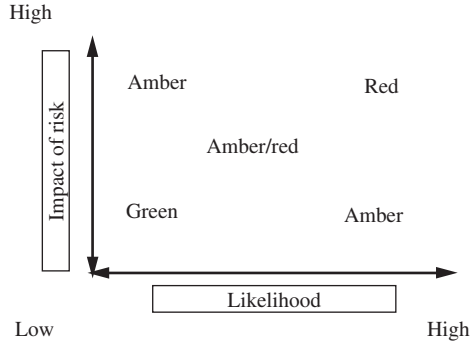


FIGURE 3.13 Risk scoring.

TABLE 3.1 Risk reports.

Department	*Activity and date reviewed*	*Risk: Red, Amber Green and risk category code*	*Action plan*	*KPIs and review*	*Risk owner*

summary version that gives the activities, risk rating, code (red, amber, green), owner and action required, using a suitable reporting tool in Table 3.1.

The risk-management policy should fit into the policy on performance management and each risk status should prompt different types of actions as a response to the risk exposure identified along, for example, the following lines:

High risk exposure – urgent board-level reports and ongoing monitoring.

Major risk exposure – director involvement – rapid review.

Significant risk exposure – manager intervention and summary briefing to director.

Moderate risk exposure – basic management practice applied.

Low risk exposure – no special action.

Trivial – review whether able to remove resources away from monitoring.

In this way, the board and top management may have a view on risk across the organization and how it is being handled. See the section on risk appetite as this will impact on the way risks are reviewed and prioritized. There may be need for a validation procedure to ensure that each risk register is valid and this is something that the CRO would address. Note that there are some internal auditors who consider this validation of risk-management practices a useful way of applying the audit resource.

Risk Categories

Each organization will have their own interpretation of risk. And this interpretation will fit the market, culture and mission of the organization in question. To help align the risk-management process with the organization's systems and procedures many organizations capture risk in a structured manner, via a set of categories that suit them. We can review some of the well-known published risk guides and consider the prompts they contain on categorization. The original King report suggests several general headings as a start to addressing the company's exposure to at least the following: physical and operational risks, human resource risks, business continuity and disaster recovery, credit and market risks and compliance risks. The Australian/New Zealand models (AS/NZ 4360:1999) identify eight categories of risk:

1. commercial and legal relationships
2. economic circumstances
3. human behaviour
4. natural events
5. political circumstances
6. technology and technical issues
7. management activities and controls
8. individual activities.

The National Audit Office's report, Supporting Innovation: Managing Risk in Government Departments, mentions the risks that are most commonly identified by departments:

- financial risk
- project risk
- compliance risk
- reputation – risks to
- missing an opportunity (e.g. exploiting IT solutions).

Internal Auditor magazine has included an article on 'Categorizing risk', which was edited by James Roth and Donald Espersen. The risk categories covered include:

- **ASSETS** – investment/credit risk, counter party risk, fraud/misuse, intellectual capital, sensitive information.
- **OPERATIONAL** – process/service quality, inefficiency, business interruption, strategic alliances/partners.
- **INFORMATION TECHNOLOGY** – business interruption, information/data quality, obsolescence.
- **REGULATORY** – regulations, applicable laws, contract risk, governance.
- **MARKET** – interest rate risk, liquidity, foreign exchange, capital adequacy.
- **STRATEGIC** – customers/stakeholders, competition/media, economy, pressure to meet goals/resources, co-ordination/communication.

The Treasury's *Strategic Risk Management* guide has adopted a different set of categories to cover the following areas:

- **EXTERNAL** – infrastructure, economic, legal and regulatory, environmental, political, market, act of God.
- **FINANCIAL** – budgetary, fraud or theft, insurable, capital investment, liability.
- **ACTIVITY** – policy, operational, information, reputational, transferable, technological, project, innovation.
- **HR** – personnel, health and safety.

CIPFA's risk categories are broken down into a mnemonic, APRICOT, which stands for:

- **ASSETS** – buildings/contents/material
- **PEOPLE** – personal security/safe working systems
- **REPUTATION** – poor media coverage
- **INFORMATION**
- **CONTINUITY OF OPERATIONS**
- **TARGETS** – failure to meet.[45]

The IIA's Handbook Series, *Implementing the Professional Practices Framework*, reinforces the change in focus when considering different types of risks by suggesting that:

> Risk assessments that capture only traditional, financial hazards are increasingly useless in today's business environment. More often than not, it is the soft, intangible issues such as human resources, integrity, reputation, and information quality that prove truly detrimental or advantageous to the organisation. (page 98)

Key Developments

When considering risk categories outside the actual business line in question, we may note several key developments for external risk including:

1. Duty of care Employers owe a duty of care to their staff – employers are expected to carry out risk assessment on the possibility of their employees perpetrating acts of negligence and other torts committed in the course of their employment. At the same time, employees owe a duty of care to the general public and their customers. And the Health and Safety at Work Regulations 1992 require employers to carry out a risk assessment for each employee to consider the risks posed by the employee's duties and environment, with regard to their individual characteristics. Birmingham City Council paid £67,000 for an employee who suffered mental stress because she was overworked in a position for which she had received no proper training. Employers must consider the welfare of their employees and the risk of injury, both mental and physical, in the workplace. Neil Hodges has noted that corporate killing is now on the government agenda, although there are no laws yet on the statute books despite the long list of disasters that include:

- *Herald of Free Enterprise* – 1987 Zeebrugge to Dover – over 200 people died with verdicts of unlawful killing in 187 cases.
- *Southall Rail Crash* – September 1997 – 7 people died and 151 injured.
- Great Western Trains fined £1.5 m for health and safety offences in July 1987 for a serious fault of senior management leading to health and safety risks.
- *Kings Cross Disaster* – 18 November 1987 – a fire at the underground claimed 31 lives.
- *Piper Alpha* – July 1988 – oil platform disaster in the North Sea caused 167 deaths.
- *Clapham Rail Crash* – 12 December 1988 – 500 injured and 35 deaths were caused when three rush hour trains collided after a signal breakdown.[46]

2. E-commerce The failure rate of Internet start-ups is high because many owners do not follow usual business practice and may be too geared towards risk taking without considering the need for suitable controls. Many organizations fail to fully appreciate the risks of cyber crime including hacking and external attacks on e-business ventures. The IIA.Inc.'s Professional Practices Pamphlet 97-1 (*Electronic Commerce and the Internet*), 1997, states in its executive summary that:

> information technology (IT) has spawned a revolution the likes of which has never been seen before. As we move from managing data to managing knowledge, the Internet will continue to have dramatic effects on people and businesses everywhere. The Internet is the latest phenomenon in the information technology arena to be introduced into our culture. The speed with which it has been adopted by both the public and the business arena indicates that perhaps

> more than any other single IT development, the Internet has the potential to make the radical changes in the way we receive information, conduct business, and even how we think.

Risk classification will suit the environment within which the organization operates. British Telecom has developed their examination of e-risk using seven categories that, in summary, cover:

- **Software** – loss or corruption.
- **Physical assets** – loss or damage to PCs, servers, media, etc.
- **Data** – loss or corruption of internal and customer data.
- **Intellectual property** – loss of patents, software, copyright, knowledge.
- **Reputation** – damage to rep from poor customer service, security incidents.
- **Liability** – internet-related, such as defamation, contractual liabilities.
- **Regulatory** – breach of regulations and DP Act.[47]

3. Fraud Fraud can pose a major risk to business and the ICAEW Audit and Assurance Faculty third annual report for 2000–2001 said that fraud is a crime increasingly linked to corruption and money laundering and conducted by organized criminals. Home Office estimates fraud at £14 billion a year.

4. Corporate reputations Reputation management is another topical risk area and this tends to be the culmination of the way an organization has managed all the other risks to its business. *Accounting and Business* magazine reported on the crucial role that reputation management has in the sustainability of a business:

> Ten years ago, the independent manufacturing company had to recall 160 m of its distinctive green bottles from around the world after traces of benzene were detected in the water. But the company failed to communicate news of the contamination quickly enough and did not carry out a speedy recall. The consumers fled the market and Perrier's sales plummeted. An advertising campaign then followed to assure consumers that the water was safe. But, the brand suffered as did the company, which was taken over by Nestle in 1992. 'The problem with Perrier was that it didn't act sufficiently quickly enough to withdraw its products. It allowed rumours to fester, and consumers lost confidence,' explains Blackett (Group Deputy Chairman of Interbrand). 'In such a crisis, companies need to be seen to act instantly in the interests of consumers.'[48]

Reputation is seen by many as a bottom line concept where all risks that an organization fails to manage properly eventually impact on its standing in the marketplace. Andrew Chambers has described the importance of this issue:

> If today's approach is risk management, Chambers believes tomorrow's will be 'reputation management. He said: 'Reputation is now moving up the agenda of enterprise management and internal auditors now need to be up-to-speed with appropriate awareness and audit approaches.'[49]

5. MIS Risk management is about selecting the right course of action based of good information that reflects all relevant circumstances and changes. Management information systems (MIS) can lead to tremendous risks where they are not reliable and robust and they should really subscribe to three facets, that is they are based around confidentiality, integrity and availability.

However, the underlying data may not always be accurate as shown by a study of business spreadsheets by KPMG Management Consulting in London, which revealed that:

- 95% of models reviewed contained major errors. Errors that could affect decisions based on the results of the model.
- 92% that dealt with tax issues had significant tax errors.
- 75% had significant accounting errors.
- 59% were judged to have poor model design.[50]

6. Communicating risk Communicating risk is a major issue in the society. This includes risks to shareholders' investments and risks to the general public. There are greater calls for companies to disclose risks more fully and so help people align their risk appetite with the company that they are considering investing in. New share offers should make it clear what is at stake and may, for example, provide some warning that it is embarking on high-risk, high-return ventures and that the readers should be aware of the commercial reality of this strategy. Quite often, communications strategies revolve around the subtle difference between warning people and scaring people. For public risk, there are several issues that can come together and shake people up. These issues have been called 'fright factors' by Peter Bennett where the risk is seen to include the following features:

- involuntary;
- inequitably distributed;
- unfamiliar or novel;
- man-made rather than natural;
- hidden and irreversible;
- particular danger to small children, pregnant women or future generations;
- arousing a particular dread;
- identifiable rather than anonymous victims;
- poorly understood by science;
- subject to contradictory statements from responsible source.

> . . . events to do with risk can be likened to a stone dropping in a pool. Sometimes there is little more than the initial splash; sometimes the ripples spread far and wide. In may cases the indirect effects – caused, as it were, by the distant ripples spread far and wide – can far exceed the direct ones.[51]

The Department of Health has established a guide to *Communicating about Risk to Public Health* which suggests that:

- messages are usually judged first by whether their source is trusted,
- intentional communication is often only a minor part of the message actually conveyed,
- responses to messages depend not only on content but also on the manner of delivery, especially emotional tone,
- experts no longer command automatic trust, no matter how genuine their expertise,
- trust is generally fostered by openness, both in the sense of avoiding secrecy and in being ready to listen.[52]

Apart from setting standards on managing risk, HM Treasury has also prepared a risk-management framework for itself. This sets out what it is doing in respect of this issue and selected extracts from the components of the 2001 framework include:

- Development of options and plans for dealing with and responding to the range of events and variables.
- Learning from experience through post hoc analysis of the development of policy and assessment of the Treasury's and others' response to events.
- Ensuring that we have the staff and systems in place to identify and assess risk resilience.
- The Treasury's policies include a variety of measures for managing risks and improving resilience to shocks. Transparency and prudence are key strategies in this respect.
- Transparency ensures that a wide range of analysis is brought to bear on an issue, reducing the risk of error . . . Prudence ensures that there is sufficient leeway to manage downside risks if they arise . . .

> The Treasury is working to strengthen further its business planning process as part of the Civil Service agenda. In the course of business planning, Treasury managers will gain assurance about the identification, assessment and management of risks attaching to key policies, objectives and processes. This will supplement other means of review, such as the work of the department's Internal Audit Team.[53]

The ICAEW calls for better communication of risk and their President Peter Wyman has said:

> The institute sees very important benefits for companies in providing better information about what they do to assess and manage key business risks. This will give practical forward-looking information and will reduce the cost of capital. It will help investors and others understand the key risks inherent in the business. Also, it will improve accountability for stewardship, investor protection and usefulness of financial reporting . . .

The ICAEW recommends:

- Enhanced risk reports will help listed companies obtain capital at the lowest possible cost.
- Listed company annual reports should contain information about risks in the broadest sense, about actions to manage them and relevant measures.
- As a backdrop for communicating about risk, companies should present their overall strategy and their process for developing it.
- Directors should communicate clearly what actions they are taking to manage these risks, providing sufficient information to allow investors to make a judgement about the risk being undertaken by the company.
- When reporting performance, directors should report promptly and in a balanced way.[54]

3.8 Control Self-assessment

The success of enterprise-wide risk management depends on an integrated process for ensuring that risks are assessed and managed across an organization in a dynamic and meaningful way. There are many techniques for reaching all parts of an organization so that self-assessment by front line staff becomes the norm. Some argue the widespread use of questionnaires that are completed by key employees as a way of assessing whether there are operations that are at risk and whether controls are addressing these risk areas properly. Another technique is the use of interviews with managers in particular business units to gauge whether the area is under control or not. A further approach is to commission comprehensive reviews of risk in high-profile parts of the organization normally by the use of external consultants, who would report back on any problems found. These three techniques are fairly straightforward, in that they involve a process superimposed on the normal business operations and support services. Unfortunately, they reinforce the ad hoc

silo approach and appear as one-off exercises carried out by a special purpose head office team. A more popular approach is the use of control self-assessment workshops, or what some call control and risk self-assessment (CRSA) workshops. The UK's CRSA Forum consists of a network of CRSA practitioners and interested persons who have formed a group that meets every quarter. Their mission is: 'Sharing, progressing and promoting best practices in self-assessment of control and risk in all organisations'. At each meeting there are normally a couple of presentations by group members on the way CRSA is operated in the organization in question. (See Appendix B for a *Best Practice* guide issued by Paul Moxey of the CRSA Forum.) Proponents of CRSA are convinced that the only way to get risk management into the heart and minds of the organization is to get everyone involved in a participative manner. CRSA may be known by a variety of different names in different organizations. In some companies, the terms *risk* and *control* do not inspire people and other more friendly terms are applied to the workshops. Note that the technique is dealt with in Chapter 5 on the audit approaches. Here we simply mention the key principles relating to CRSA as part of the risk-management system. An article by Paul Makosz in *CSA Sentinel* outlined the development of the CRSA approach:

> While I was at Gulf Canada Resources, we began to recognize that the heart of many problems lies in a corporate culture that could directly affect the bottom line; but we unfortunately had no tools to help us in identifying major risks before they became problems. Bruce McCuaig, my predecessor at Gulf Canada Resources, originated the CSA idea. He had been studying Watergate related issues at the parent company, Gulf Corp. About the same time, a serious management fraud had been discovered in a Gulf Canada subsidiary, although the internal auditors had been there only recently. Bruce kept asking, 'What's the point of auditing the little things if the culture is wrong-headed?' Gulf was going through some team productivity exercises at the time, so Bruce wanted to teach teams about internal control and have them self-assess their position. The rest is history. Bruce and I wrote about it in 'Ripe for Renaissance,' an article that appeared in the December 1990 edition of Internal Auditor.[55]

The important point to note in this section is the need to blend the CRSA technique into the risk-management process generally. A staged approach can be applied to this end as illustrated in Figure 3.14.



FIGURE 3.14 A staged approach to risk.

Stage One – General Interest

There are no organizations that have not come across the concept of risk management and at the outset there would tend to be pockets of interest in the idea of recognizing and dealing with risk. Specialist staff such as health and safety people, project managers, insurance officers, IT security staff and finance people will tend to have a good understanding of the way risk assessment can be used to direct resources more efficiently, but only in the context of their very specialist areas of work. For example, health and safety officers have always used risk assessments to isolate aspects of work that need to be prioritized for various protective and preventive measures. Likewise project teams would have an in-built assessment of risk to form risk registers that will contain issues that will have to be addressed for the project to run smoothly and deliver results. Organizations at stage one will contain isolated pockets where risk assessments are regularly undertaken by specialist staff, but just for their area of interest.

Stage Two – Rumblings of Research

An organization reaches stage two when people within some of the departments start to look into the topic of risk management outside of the specialist roles mentioned at stage one. This developing interest is normally initiated by finance staff who recognize that risk assessment supports the way financial controls are developed into robust systems of internal control. Most regulatory regimes in both the private and public sectors require the maintenance of adequate systems of internal financial controls, and more often, external reporting of these controls in the annual report. Bombarded by recommendations from the external and internal auditors, along with the trend towards the use of financial handbooks and finance procedures/regulations, the accounting people tend to feel comfortable with the idea of risk management and effective internal financial controls. Stage two organizations contain people who have started to pull together best-practice guides and other publications relating to risk management for finance and some of the general managers.

Stage Three – Responsible Person

An organization arrives at stage three when it is prepared to resource the drive towards formal risk management. This is really about assigning responsibility in the organization for pulling together efforts to address risk in various operational areas and support services. Again, this newly found role would tend to be given to a senior finance manager – since generic risk assessment would be seen as a finance-related issue to support any internal control statements in the annual accounts. The good news for stage three entities is that someone is starting to co-ordinate the risk-related activities and achieve some kind of structure.

Stage Four – Top Management Interest

An organization arrives at stage four when risk and risk management becomes a boardroom agenda item. Where the board decides to set policy and strategic direction for the way risk is addressed by managers and their staff, the risk-management process starts to take on a clear form, even if this is only in terms of a sense of direction and commitment. Stage four organizations contain directors and senior managers who make clear statements about the need to address

risks in the way strategy is developed and the way operations deliver. A formal risk policy will appear as part of the key corporate messages that hit the top-down communications process.

Stage Five – Awareness Seminars

Hollow messages from the top can communicate one-line concepts, but are not very good at delivering changes in working practices. This calls for new thinking and a sound learning process that makes a difference. Major change initiatives call for a structured way of getting the message across with a hands-on format that reaches key staff in a systematic and planned manner. Stage five organizations will tend to provide awareness events where people are told about risk-management initiatives and how it affects them. If an organization is not prepared to resource efforts to bring risk awareness to select managers across the organization, then there is less chance of driving home an initiative that involves new ways of thinking about old problems. Bringing different parts of the business together in this way forms the basis for an enterprise-wide risk-management approach.

Stage Six – Infrastructure Build

When people understand the way risk management can be used to help ensure objectives are achieved, the organization can step into stage six. Here, it starts to develop a process for assessing risk across key parts of the business and reporting the results up into an assurance reporting mechanism, which eventually hits the published internal control statement. Most organizations will amend the reporting process that has been used to deal with financial controls and extend it across front line operations, while trying not to retain the emphasis on finances. In stage six organizations, the risk policy becomes more of a risk-management strategy that reaches into key parts of the business as well as support services. Moreover, such efforts are often overseen by a suitably formulated audit committee. In this way, stated intentions can be turned into real actions. One key aspect of the infrastructure build is the adoption of a suitable control model such as COSO. If there is no model of control to form the basis of the implementation of control self-assessment, it is like buying a car before ensuring there are suitable roads to drive the car along.

Stage Seven – Risk Exercises

It is only when an organization has gone through a version of stages one to six that it can turn to stage seven, where teams, projects, operations and support functions can start to review their work areas. What is commonly referred to as control self-assessment or control risk self-assessment workshops fit in at stage seven. Here, top-down direction on risk and high-level discussions at middle management level can be met with bottom-up information about the state of operational risks and associated controls.

Stage Eight – Integrated

The final stage relates to the integration of all risk efforts into the way the organization plans strategy, sets performance measures and makes decisions to close gaps between actual

performance and targets. In this scenario, there needs to be expert guidance in bringing together the various strands of risk-based activities and resulting risk registers, action plans and reports to form an overall assurance reporting process. Most see this as a role for a formally appointed CRO, who has high-level representation and reports to the board. Some would argue that the CRO post should ideally appear at stage one to guide and drive the organization through the remaining stages as an effective system of risk management is built, implemented and then embedded into the culture of the workplace.

The eight-stage model is useful in assessing where an organization stands before embarking on an audit consulting role, since the required input will vary depending on which stage the organization currently sits. Getting managers and staff together into workshops and asking them to identify their objectives, risks and controls (or risk strategies) many times falls flat on its face. Because the wrong strategies have been applied at the wrong time and the organization has not been through the development stages. Each stage requires different drivers:

Stage one – general interest: build on the interest and focus it into a pro-organizational drive to get different specialist teams talking about their approach to risk management.

Stage two – rumblings of research: develop a database of best-practice guidance and find out what others in the business sector are doing. Construct a checklist of matters to be addressed in formulating and implementing a corporate risk policy.

Stage three – responsible person: define respective roles and responsibilities, in particular a champion for the cause who can set a direction for the organization.

Stage four – top management interest: secure a sponsor on the board who can ensure risk management sits firmly on the corporate agenda. One way is to get the board (and audit committee) to carry out their own assessment to arrive at their top ten risks to start the process.

Stage five – awareness seminars: it is most important to get key players around the organization together in a series of events to provide understanding, promote buy-in and ensure each manager accepts that they have a clear and direct responsibility for managing risks in their areas of responsibility.

Stage six – infrastructure build: much of this will revolve around building a suitable information system that categorizes and captures risk activities into a formal assurance reporting format. The exact risk activities will have to be decided on and whether these activities cover the entire organization or just high-profile areas.

Stage seven – risk exercises: here the organization will need to conduct surveys and/or facilitated workshops in a way that best suits the structure and culture of the business.

Stage eight – integrated: much of this will be based on defining the role and competencies of a CRO or equivalent and ensuring that the risk assessment process is revisited and updated both regularly and whenever changes impact various risk profiles.

The problem facing some organizations is that they start the eight-stage process with no clear understanding of the stage development and targets. As a result, many get stuck at an early stage and write the entire thing off as a false start. CRSA only really works where the organization has arrived at stage seven. CRSA is also discussed in Chapter 5 on audit approaches.

3.9 Embedded Risk Management

We now arrive at the pinnacle of risk-management best practice, the much-sought-after 'embedded risk management'. Again, like much of the theory of risk management, it sounds simple as an ideal and Turnbull includes among the criteria to assess the internal control framework (monitoring arrangements) the following question:

> Are there ongoing processes embedded within the company's overall business operations, and addressed by senior management, which monitor the effective application of the policies, processes and activities related to internal control risk management? (Such processes may include control self-assessment, confirmation by personnel of compliance with policies and codes of conduct, internal audit reviews or other management reviews.)

Meanwhile the Treasury's *Strategic Risk Management* guide recognizes a similar need to integrate risk into the organization by suggesting that: 'The embedding of risk management is in turn critical to its success; it should become an intrinsic part of the way the organization works, at the core of the management approach; not something separated from the day to day activities.'

We could go on. Most risk standards, guides, aids and commentary contain the phrase (or an equivalent term) *embedded risk management*. Gordon Hill warns about trying to do too much too quickly:

> Integration with existing process is as important but presents different challenges purely because the process will be operational. You could embark on a programme of reviewing all processes for risk. However, I would guard against this approach on the basis of 'if it ain't broke don't fix it'. Wait until there is a problem within a process that suggests changes are needed; this is the time to introduce risk assessment and this will ensure the greatest value is delivered. If benefit is provided then staff will understand the value of risk intervention . . . Attacking everything at once is not a practical solution. Organizations need a way of deciding where to integrate and when. Using a properly prioritized risk register to focus on the biggest issues is the most effective way of targeting effort. This way the organisation will achieve the fastest payback and the greatest commitment and will have in its grasp a route map to the managed risk culture.[56]

Meanwhile we can complete our risk model by putting in the remaining component of effective risk management, with a view to tackling the need to get risk firmly inside the organization's processes. By adding several factors consisting of three black boxes (ERM/CRSA, SIC and Stakeholders) and four grey boxes (time, cost, values, embed) we can achieve a fully developed model of effective risk management in Figure 3.15.

Starting with the black boxes first, these additions are explained below:

ERM/CRSA As discussed above, there should be a process that ensures risk is understood, identified and managed at grassroots level ideally through a form of control risk self-assessment programmes. Meanwhile, there should be a further process for ensuring risk assessment is undertaken throughout key parts, if not all, of the organization and that it is driven from the top and runs down, across and throughout all levels of management. The CRO would help co-ordinate these efforts.

SIC The risk efforts and ensuring controls should feed into the SIC that each larger organization should formally publish. The inputs to the annual SIC should arrive from suitable assurance reporting systems (perhaps revolving around local and aggregated risk registers).

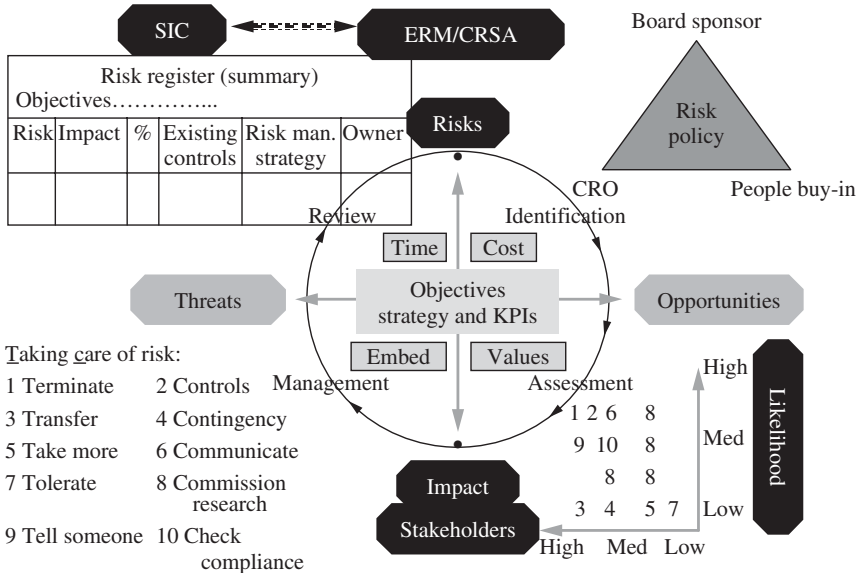


FIGURE 3.15 Risk management (10).

Stakeholders The organization should have a formal process for communicating with stakeholders the efforts of the risk-management system and any information that gives value to various interested parties. The risk-management system should address the concept of risk tolerance and make clear what areas are likely to pose a threat to the organization, or the general public where appropriate and the extent to which strategies and performance targets are likely to be fully achieved. Much use can be made of the Internet website to communicate risk publicly. The Lord Chancellor's Department has a website account of its Risk Management Framework for 2002 and under 'communication' states that:

> Communication with stakeholders in the identification and the management process is paramount. Communication should educate the public on the risks they may be exposed to; on the different ways in which the risks can be managed; on the Department's objectives in the management of risk; and in individuals' own role in managing that risk, where the decision is taken to avoid government legislative intervention. It is also, though, about the gathering of information to assist in decision making in the centre. This must include using communications to develop an understanding of how messages about risk will be received in the light of knowledge and values which members of the public bring to bear in framing their interpretation of and response to the messages.[57]

Time The risk model is based on doing more to research, analysing and addressing risks that impact the organization and ensuring there is transparency and competence in the way these risks are addressed. The task does create a challenge and provides additional considerations for the board, senior and middle management and work teams, as well as grassroots operatives. Effective risk management depends in part on the time that is made available. Getting people together for awareness seminars and getting them into teams to assess their operational risks take time. Working out the logistics for a workforce to meet up where people are scattered throughout

the country and communicate through the e-mail system and the corporate intranet can be near on impossible. In this example, time is needed to find a solution where risk workshops may be arranged with select representatives of the workforce and perhaps others who should be involved, rather than trying to get everyone into these workshops. Or to base the exercises around common processes where a member from each location joins a workshop to assess the risks inherent in the process in question. Questionnaires may be used as a start where it is hard to get people together, and maybe use break-out groups at the next staff conference rather than try to set up separate events. Team and staff meetings can be used to kick off the risk assessment process again in recognition of the lack of time. The best approach is to define the benefits of risk management and then make space to conduct risk exercises. Where we have got closer to embedding risk into company processes, it may just be a matter of ensuring basic tasks such as planning, target setting, corporate restructuring, key decision making, performance management, project planning, procedure design, new ventures, partnering opportunities, new products and so on are only agreed when a formal assessment of risks has been undertaken and recorded.

Cost This factor is linked to time. It does cost money to implement new ideas even where we are building these ideas into our existing systems. External expertise may be required in the early days of establishing risk management to ensure ideas can be turned in practice. Information systems may be updated to build in the risk factor and capture the results of any relevant exercises. Where the CRSA approach is adopted, we will need to book accommodation and support services such as electronic voting systems (where used) and good facilitators and recording systems. The board-level support for risk management needs to be matched with a proper delegated budget, ideally located with the CRO. Policies with no defined funding attached to them tend to end up as paper documents with no real value.

Values The best way to establish risk management is to avoid just delivering a set of regulations in the form of things that must be done to satisfy the policy requirements. It is better to have as an objective the need to instil an acceptance that risk management is an important aspect of the business and it should be part of the values that people within the organization subscribe to. Decisions should be taken without rushing headfirst into unmarked waters or holding back and resisting all suggested changes, but they should be made after having undertaken a formal assessment of key risks and in conjunction with a strategy for dealing with unacceptable risks. It is more about the way people behave at work and achieving a balance between recklessness and stagnation. In other words, the value system needs to recognize everyone's accountabilities and responsibilities as well as the need to surge ahead in innovative ways.

Embed The final part of the model falls out of all the other components and consists of the bottom line concept of embedding risk management into and inside the organization. Most of the points on embedding risk management have already been covered and it only remains to provide a graphic illustration from America's space shuttle programme to illustrate the importance of a risk-focused culture to ensure controls do what they are meant to do:

> the unusual risks we encounter in performing space operations work demand a remarkable amount of attention to detail . . . a tiny amount of water accidentally trapped in an orbiter tile by the oil from a stray fingerprint could freeze under certain conditions, shattering the tile and exposing astronauts to reentry risk.[58]

3.10 The Internal Audit Role in Risk Management

This chapter has so far provided a brief introduction to risk management – the growing trend towards recognizing risk as a key driver for all the systems that underpin a successful organization. We now have to touch on the way internal audit fits into the risk equation. As a start the IIA Attribute Standard 1220.A3 states that internal auditors must have regard to key risks and that: '*Internal auditors must be alert to the significant risks that might affect objectives, operations, or resources. However, assurance procedures alone, even when performed with due professional care, do not guarantee that all significant risks will be identified.*'

Back in 1999, Gill Bolton issued a warning to internal auditors that they were in danger of fighting against effective risk management because they:

- Tend to recommend highly risk averse processes and procedures.
- Are not aware of the organisational preferences for risk taking (also known as risk appetite or risk tolerance). They are not alone in this as few organisations have properly defined risk taking preference.
- Make recommendations on a fairly ad hoc basis, often without considering the organisational impact of their recommendations.
- Fail to get sufficiently close to the strategic opportunities and challenges that their organisations are working on and working towards.
- Add an administrative burden at a time when speed and flexibility are critical.
- Do not become actively involved in major organisational change programmes.

> . . . In conclusion I do not believe that internal auditors should aim to change their role to that of the risk manager. Rather, they should work together with all other risk management and monitoring functions in their organisation to help achieve aligned and streamlined total risk management.[59]

It is clear that the rapid drive towards risk management arose partly because of prescribing codes, partly fuelled by scandals across sectors and organizations and also because successful businesses understood and addressed their key risks. This movement towards embracing risk should in no way be hindered by the internal auditor. The IIA Handbook Series on *Implementing the Professional Practices Framework* (p. 92) suggests that: 'The idea that risk must be both embraced and eliminated by the organisation runs contrary to traditional internal auditing thought. In the past internal audit practitioners have often sought only to eliminate risk.' The definition of internal auditing makes it clear that we must be concerned with risk and risk management. Moreover, there are several IIA professional standards that drive home the importance of internal audit involvement in the organization's system for managing risk. Performance Standard 2120 makes it clear that:

> The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.
>
> ***Interpretation:***
>
> Determining whether risk management processes are effective is a judgment resulting from the internal auditor's assessment that:
>
> - Organizational objectives support and align with the organization's mission;
> - Significant risks are identified and assessed;

- Appropriate risk responses are selected that align risks with the organization's risk appetite; and
- Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.

Risk management processes are monitored through ongoing management activities, separate evaluations, or both.

2120.A1 – The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the:

- Reliability and integrity of financial and operational information.
- Effectiveness and efficiency of operations.
- Safeguarding of assets; and
- Compliance with laws, regulations, and contracts.

A ground breaking Professional Briefing Note number Thirteen issued by the IIA.UK&Ireland (1998) addressed internal audit's role in managing risk. Some of the key points made in the briefing note have been summarized below:

It is increasingly recognised, however, that internal audit needs to add value to the organisation by closely aligning itself with the major concerns of senior management and focusing on those issues that are critical to success. An internal auditor's responsibilities are similar to those of a consultant. They are responsible for the technical quality of the advice that they give. But it is management's decision whether, or not, to accept that advice in the light of its fuller understanding of the situation. Internal auditors' involvement in assessing risk or identifying controls including:

- Facilitators enabling and guiding managers and staff through the process . . .
- Team members who are a part of broader based groups . . .
- Risk and control analyst providing manager with expert advice . . .
- Proving tools and techniques used by internal audit to analyse risks and controls.
- Becoming a centre of expertise for managing risk.

The problem of how the need for audit objectivity and independence can be squared with the demands of management for professional advice and assistance, as well as the necessity for internal audit to be perceived as value-adding is not, in itself, new.[60]

The need to balance independence and the assurance and consulting roles of internal audit is a growing feature of the new look internal auditor. The value add equation means we cannot ignore the need to help as well as review. Some argue that internal audit needs to reposition itself at the heart of the risk dimension and drive through the required changes. In a recent study funded by IIA.Inc. titled Enterprise Risk Management (ERM): Trends and Emerging Practices, Tim Leech asks the profession to get to grips with ERM and has questioned whether internal audit departments will help or hinder the ERM movement:

We believe ERM will become an integral part of the management process for organisations of the 21st century. It will influence how organisations are structured, with some appointing a chief risk officer that reports to the CEO or board of directors. It will influence how strategic planning

> is done. And it will certainly influence how internal auditing is performed. This conclusion may come as a shock to many internal auditors who do not even know what the term ERM means, let alone play a significant role helping their clients implement ERM systems. Numerous other studies released over the last few years are unanimous – ERM is vastly superior to traditional 'silo based' approaches to risk and assurance management . . . Traditionalists defend the status quo on the grounds that the silo approach to audit is necessary to maintain 'auditor independence'. As long as internal auditors think their job is to decide what constitutes 'adequate' control on a fraction of the risk universe, instead of reporting on the quality of the risk assessment processes and the reliability of management representations on risk status to the board, true audit independence will not exist. I encourage internal auditors to consider whether they are helping or hindering the adoption of ERM. What is becoming increasingly obvious is that internal audit practitioners that do not get behind the ERM movement may soon see it roll right over them. Make sure you are on the right side as the ERM movement gathers momentum.[61]

This viewpoint represents an important challenge for the internal auditor who has been asked to champion the risk movement while retaining the independent assurance role. Models are available to help in the key decisions underpinning the new look internal audit role. Practice Advisory 2120-1 on Assessing the Adequacy of Risk Management Processes gives an interpretation of standard 2120 (the internal audit activity must evaluate the effectiveness and contribute to the improvement of risk-management processes):

> Determining whether risk management processes are effective is a judgment resulting from internal auditor's assessment that:
>
> - Organizational objectives support and align with the organization's mission.
> - Significant risks are identified and assessed.
> - Appropriate risk responses are selected that align risks with the organization's risk appetite.
> - Relevant risk information is captured and communicated in a timely manner across the organization,
> - enabling staff, management, and the board to carry out their responsibilities.

Risk-management processes are monitored through ongoing management activities, separate evaluations, or both.

> 1. Risk management is a key responsibility of senior management and the board. To achieve its business objectives, management ensures that sound risk-management processes are in place and functioning. Boards have an oversight role to determine that appropriate risk-management processes are in place and that these processes are adequate and effective. In this role, they may direct the internal audit activity to assist them by examining, evaluating, reporting and/or recommending improvements to the adequacy and effectiveness of management's risk processes.
> 2. Management and the board are responsible for their organization's risk-management and control processes. However, internal auditors acting in a consulting role can assist the organization in identifying, evaluating, and implementing risk-management methodologies and controls to address those risks.
> 3. In situations where the organization does not have formal risk-management processes, the CAE formally discusses with management and the board their obligations to understand, manage and monitor risks within the organization and the need to satisfy themselves that there are processes operating within the organization, even if informal, that provide the appropriate level of visibility into the key risks and how they are being managed and monitored.

4. Understanding of senior management's and the board's expectations of the internal audit activity in the organization's risk-management process. This understanding is then codified in the charters of the internal audit activity and the board. Internal auditing's responsibilities are to be coordinated between all groups and individuals within the organization's risk-management process. The internal audit activity's role in the risk-management process of an organization can change over time and may encompass:
   - No role.
   - Auditing the risk-management process as part of the internal audit plan.
   - Active, continuous support and involvement in the risk-management process such as participation on oversight committees, monitoring activities, and status reporting.
   - Managing and co-ordinating the risk-management process.
5. Ultimately, it is the role of senior management and the board to determine the role of internal auditing in the risk-management process. Their view on internal auditing's role is likely to be determined by factors such as the culture of the organization, ability of the internal audit staff and local conditions and customs of the country. However, taking on management's responsibility regarding the risk-management process and the potential threat to the internal audit activity's independence requires a full discussion and board approval.

Audit should determine the effectiveness of management's self-assessment processes through observation, direct tests of control and monitoring procedures, testing the adequacy of information used in monitoring activities and other appropriate techniques. Gregg R. Maynard has provided a succinct list of ways that internal audit can respond to the risk agenda:

1. Combining objective and subjective analysis of the audit universe to reveal audit priorities. Moving away from the audit cycle – quantitative measures then qualitative ones that change as circumstances change.
2. Analyzing management's ability to achieve its stated goals and objectives in pre-audit narratives. Management's assessment of risk and tolerances.
3. Using questionnaires to examine internal controls from the top down. Explore the tone at the top – ethical standards, strategic planning, management information and risk management.
4. Analyzing the processes for establishing and overseeing risk limits. Threshold and set limits and financial and operational targets.
5. Reviewing other risk management functions, such as treasury, compliance, and accounting control. Base reliance on assessment and also get the big picture on risk exposures.
6. Observing the strategic planning process and its results. Look to audit the future and changing risks but not in a decision making capacity.
7. Evaluating strategic initiatives. Eg strategic alliances and new projects.
8. Integrating audit activities. Eg IT audit and front line audit.
9. Basing the audit process on the net effect of risk exposures and compensating controls. Audit recommendations should be based on this equation – risks less controls. Then determine the extent of substantive testing needed to confirm the position.
10. Partnering with management by providing consulting services and value added information.
11. Reviewing ethics as a basic element of internal control.
12. Conducting a comprehensive audit of the entire risk management program.[62]

Internal auditors must add value to an organization and IIA Performance Standards 2100 covers the nature of internal audit work:

The internal audit activity must evaluate and contribute to the improvement of governance, risk management, and control processes using a systematic and disciplined approach.

2110 – Governance

The internal audit activity must assess and make appropriate recommendations for improving the governance process in its accomplishment of the following objectives:

- Promoting appropriate ethics and values within the organization;
- Ensuring effective organizational performance management and accountability;
- Communicating risk and control information to appropriate areas of the organization; and
- Coordinating the activities of and communicating information among the board, external and internal auditors, and management.

2110.A1 – The internal audit activity must evaluate the design, implementation, and effectiveness of the organization's ethics-related objectives, programs, and activities.

2110.A2 – The internal audit activity must assess whether the information technology governance of the organization sustains and supports the organization's strategies and objectives.

2110.C1 – Consulting engagement objectives must be consistent with the overall values and goals of the organization.

The Treasury (*Strategic Risk Management*) has echoed the IIA guidance on proactive involvement from internal auditors and their guide to risk management suggests that:

> Internal audit may be used by management as an expert internal consultant to assist with the development of a strategic RM process for the organisation . . . However it is important to note that the function of internal audit is to give an independent assurance about the way in which it is controlled; it is neither a substitute for management ownership of risk nor is the presence or activity of internal audit a substitute for an embedded review system carried out by various staff who have executive responsibility for the achievement of organisational objectives.[63]

This need for clarity of role definition has been explored by Andy Wynne who has argued that:

> The Turnbull report claims that the 'main role of internal audit is to evaluate risk'. It is not. Internal auditors should only review the extent that managers and board members have identified, evaluated and managed the company's risk and 'monitor the effectiveness of the system of internal control' that has been introduced to address the significant risks. The evaluation of risk is a key management task. It is a subjective assessment that should not be delegated to business advisors.[64]

Meanwhile, the 2002 Position Statement from the IIA.UK&Ireland discusses the internal auditor's responsibilities on risk and considers the concept of risk-based auditing as:

> an approach that focuses on the response of the organisation to the risks it faces in achieving its goals and objectives. Unlike other forms of audit it starts with risks rather than the need for controls. It aims to give independent assurance on the management of risks and 'to facilitate improvements where necessary'. The scope of audit assignments undertaken and the priority given to them should be determined by risk, taking full account of the organisation's own view of risk.[65]

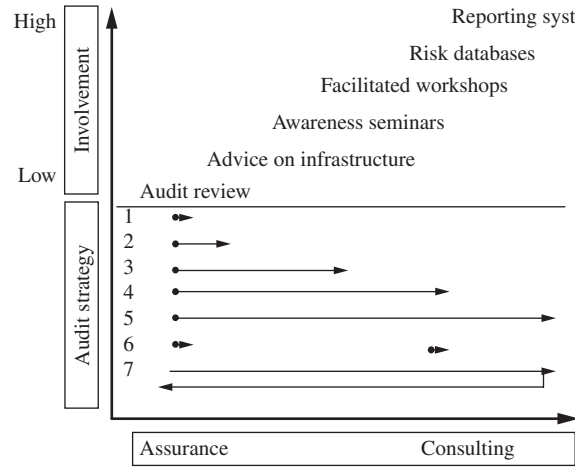


FIGURE 3.16 Assurance and consulting services.

It is possible to sum up the audit role in risk management by using a new model in Figure 3.16.

Before we go through the Assurance and Consulting Services model, two key points need to be made. First, reviews are more reliable where the reviewer is impartial. Second, value add means contributing specialist expertise to promote corporate success. When an organization needs to get a risk-management system up and running, and looks to the auditor for help setting up, it is hard for the same auditor to then give an impartial assurance on this same system. At first sight, the two concepts are incompatible. There are, however, various ways that this apparent inconsistency can be managed. The model that we are using has seven approaches:

1. The standard audit review approach is adopted. Here, the internal audit team monitors the way systematic business risk management is established and implemented, and then goes on to review whether it is reliable, robust and meets the needs of the organization. In turn, internal audit is able to furnish independent assurances to the board on the state of risk management.
2. This is similar to approach one, with the addition of ad hoc advice and guidance provided on request. Internal audit may make presentations to the board and turn up to meetings or workshops where risk management is being discussed and decided on, and make contributions as required.
3. Approach three takes things a step further and the internal auditors start to get involved in raising awareness. The main feature here is that internal audit would lead various seminars and events that promote corporate governance, risk management and control.
4. The next level is where internal audit facilitates CSA workshops and takes the risk message to the grassroots across the organization. Auditors bone up on facilitation skills and lead work teams, projects teams or process-based work groups and help the teams prepare suitable risk registers to reflect their prioritized risks and action plans.
5. Level five goes all the way. Here internal audit compiles the corporate risks database from all the risk-based activities that are happening in the organization. Audit will go on to develop a reporting system that provides aggregated and disaggregated reports at appropriate levels in the organization. The assumed role is akin to that of the so-called organization's CRO.
6. The level six approach is based on establishing two separate strands to the internal audit service. The first focuses on the main assurance and review role, although this is now likely

to be risk based, concentrating on operational risks that have been identified. The second performs a consulting role in facilitating CRSA events.

7. The final approach is to play a full role in starting and developing systematic risk management across the organization to get the process going. Then, having helped set up the process, internal audit moves away from the consulting service and back to the main assurance role. In this way, the full responsibility to make risk-management work is given back to the line.

The above basic strategies can be used as a platform to fit the internal audit service into the development of risk management throughout the organization. The approach and style selected will be whatever suits the organization and the audit team in question. The internal auditing role in reviewing risk management has been recognized in the British standard on risk management:

> If the organization has an internal audit function, this may be accountable for providing the senior management with independent assurance on:
>
> - Risk management processes, both their design and how well they are working;
> - Management of key risks, including the effectiveness of the controls and other responses to these; and
> - Reliable and appropriate assessment of risk and reporting of risk and control status.
>
> The organization's risk and internal audit functions may operate independently. They should share information and coordinate their activities. The information shared may include:
>
> - Each function's annual activity plans;
> - Methods of managing risks effectively;
> - Key risks;
> - Key control issues;
> - Output from risk management process activity and audits; and
> - Reporting and management information.[66]

Auditing Your ERM Program

By Dan Swanson, Compliance Week Columnist

Everyone talks about the need for good risk-management programs, but nobody seems to know how to audit them to ensure they actually work. Who bears responsibility for setting the parameters of an ERM program is pretty clear: the board of directors and the C-level executives. They decide what the risks are, what level of risk they're willing to tolerate, and what risks they do not want to tolerate. They are responsible for monitoring and responding to ERM outputs and obtaining assurance that the organization's risks are acceptably managed within the boundaries specified. Also remember that risk management is not an end in itself; it has value only if it assists a company to achieve its business objectives over the long term. Internal auditors, in both their assurance and consulting roles, contribute to ERM in a variety of ways. They spend most of their time assessing how effectively management has responded to key risks by developing adequate operations and control structures. Fundamentally, the audit team provides the board and management with an objective assessment of the company's ERM efforts, including where the company can improve.

Why Care Whether ERM Works?

According to the Committee of Sponsoring Organizations, ERM is ''a process, effected by an entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, manage risk to be within its risk appetite, and to provide reasonable assurance regarding the achievement of entity objectives.'' Notice the process view – that is, risk management is more than a risk-management system. Or, as a friend of mine puts it, ERM is how you address uncertainty around organizational goals.

From an internal audit perspective, inadequate identification of key risks to an organization increases the likelihood of bad events occurring. Improper identification can result in wasting resources on areas of low risk with little reward. Conversely, it can leave a company more exposed to negative events. (An example from the financial industry: At banks and mortgage companies, how much of a priority did the boards place on oversight of lending activities? Not much, I'd say, and look where it got them.)

Still, even if top management effectively identifies its key risks, the company still needs assurance that its response to those risks is effective. Effective response is a crucial part of ERM, and that means attention to the design and operation of internal controls. Indeed, informal response to key risks increases your vulnerability to something going awry. Strong controls must exist and work for ERM to be effective – so, enter the internal auditor.

Risk is perfectly fine at an acceptable level, but management must define what that acceptable level is in the interest of achieving the company's goals. Using another banking example, management might challenge the board to define the point at which losses from bad loans become unacceptable. If a $1 million loan goes bad, will the board become concerned? What about a $10 million loan? The specific number tends to change over time, so the question must be asked periodically to maintain an understanding of the correct risk appetite. Furthermore, banks face many other potential causes of loss as well, and some of them cannot be expressed in pure dollar terms. (Think of the cost of adverse publicity after a customer data theft.)

An audit of ERM should determine whether significant risks to the organization are appropriately identified and assessed on an ongoing basis. It should also confirm that those risks are monitored for possible changes, that risk-management techniques (insurance, hedging, and the like) are in place, and that management has the ability to recognize and respond to new risks as they arise.

The Guts of an ERM Audit

An audit can focus solely on the effectiveness of the ERM program if you want, but it can also be extended to look at ERM efficiency. Auditors can provide assurance that information about risks and the management of them is collected, summarized, and reported properly to the appropriate level of the governance structure.

There are two distinct elements to most ERM audits: evaluating the design and implementation of the program as a management system and evaluating the operational practices of the program, including an assessment of the risks currently being managed.

In general, internal auditors should assure management and the board that everything that should be done to manage risks is being done. Auditors should also provide guidance on control effectiveness and feedback on managerial decisions and results. Further issues worth considering in an ERM audit include:

- Are the organization's risk-management efforts appropriate to its needs? This includes management's recognition of, and response to, emerging obligations and opportunities in risk management and corporate governance.
- Has an effective risk-management program been developed and implemented? Is accountability well established and acknowledged by those to be held accountable? Has management and audit agreed on the program's definition?
- Are there appropriate systems, policies, procedures, and guidelines relating to ERM, supported by suitable awareness, training, and compliance activities?
- Has the organization embraced the risk-management philosophy? Is executive management seen as a strong proponent, and is the consideration of risk an integral part of day-to-day business decisions?
- How successful are the risk-management efforts? This is a tricky question to answer given the inherent uncertainties in risk, but a retrospective review of the organization's identification of and response to risks, including incidents that indicate inadequate controls, should be revealing.
- Do we need to increase the understanding of our key risks and what else needs to be done? Have we done everything necessary to get a grip on enterprise-level risks?

Internal Audit's Role in Risk Management

The Institute of Internal Auditors proposes that risk-management activities be divided into three groups. One includes internal auditors providing assurances as discussed above. A second group includes activities exclusively related to management decisions, such as selecting risk appetite and risk responses. (This second group of risk-management activities should not be done by internal audit as they are deemed to be management activities.) The third group includes risk management activities that may be performed by internal audit when there are safeguards in place. Safeguards may be things like changing the internal audit charter to include these added responsibilities and receiving acknowledgements from management regarding their responsibilities.

Fundamentally, enterprise risk management is not a new concept. What perhaps is new is the importance of bringing risk management into the management decision-making process and ensuring a corporate view of the relationships between risks in different parts of the organization is regularly evaluated and responded to.

Risk management is inherent in every organization. Any manager or employee who have been given objectives will almost unconsciously assess the things that will prevent them from reaching their goal. At a minimum they will manage those risks in an informal ad hoc way. ERM is a high-level formalization of this natural process. As a formal process, it needs a coordinator to draw out of all areas of the organization key risks and current efforts to mitigate them. We also need to move from a focus on risk identification to a focus on how best to manage our significant

risks. Finally, the goal of risk management is not to reduce uncertainty. It is, rather, to help organizations make better decisions and to respond more intelligently when the unexpected inevitably occurs.

The bottom line: Risk management needs to be integrated into the organization's entire operations from board oversight to senior management's strategic planning and leadership to the operating management's day-to-day operational control. And perhaps this is nothing new, but certainly it is important to the organization's long-term success and worthy of a formal evaluation by internal audit.

Reprinted from *Compliance Week*. This article was originally published in Compliance Week. Reproduced by permission of Compliance Week. All rights reserved.

3.11 New Developments

In terms of risk management, the Walker review (a review of corporate governance in UK banks and other financial industry entities, 16 July 2009) made several major observations/suggestions which can be summarized as follows:

- The review points to the distinction between the responsibility of the board in the management and control of risk and decision-taking in respect of risk appetite and tolerance.
- The responsibilities of the audit committee are highlighted in terms of their oversight and reporting to the board on the financial accounts and adoption of appropriate accounting policies, internal control, compliance and other matters.
- Walker notes the potential or actual overload of the audit committee and the need for a closely related but separate capability to focus on risk in future strategy and concluded that best practice in a bank or life assurance company is for the establishment of a board risk committee separate from the audit committee.
- Alongside assurance of best practice in the management and control of known and reasonably measurable risks, the key priority is defined for the board's overall risk governance process to give clear, explicit and dedicated focus to current and forward-looking aspects of risk exposure, which may require a complex assessment of the entity's vulnerability to hitherto unknown risks.
- One major recommendation was that the bank's board should establish a board risk committee separately from the audit committee with responsibility for oversight and advice to the board on the current risk exposures of the entity and future risk strategy. The board risk committee should, like the audit committee, be a committee of the board and should be chaired by a NED with a majority of non-executive members, but additionally with the finance director (FD) as members or in attendance and with the CRO invariably present. This risk committee would advise the board on risk appetite and tolerance for future strategy, taking account of the board's overall degree of risk aversion, the current financial situation of the entity and – drawing on assessment by the audit committee – its capacity to manage and control risks within the agreed strategy.
- One further suggestion was that in support of board-level risk governance, the bank's board should be served by a CRO who should participate in the risk management and oversight process at the highest level, covering all risks across the organization, on an enterprise-wide basis, and should have a status of total independence from individual business units.

The above may well have profound implications for internal audit as the CRO assumes a much higher status in many companies and alongside increased independence and a remit to report to a powerful risk committee, the CRO may end up with higher status than the CAE. The

strains on risk management in banks and other financial institutions were obvious when the Credit Crunch traumatized the financial system in most developed economies. These strains were clearly described by KMPG when they addressed the question: is risk management permanently broken:

> In some ways, it is not surprising that organizations are struggling. The number and the complexity of the risks that investment funds have to manage today are vast and growing all the time. Against such a backdrop, many organizations' risk management systems have become overcomplicated, cumbersome, confused, inefficient, ineffective, and expensive. All too often, it is difficult for organizations to "see the forest for the trees." KPMG believes that a single, consistent risk framework, wherein all functions have a coherent, integrated view of both risk and return, is required to meet business needs and external requirements while adding value to the management process. In light of the current crisis, the question at the top of senior executives' minds is "where do we start?" One central aim of any reassessment of risk management must therefore be to simplify the system so that the three essential elements of an effective risk regime – governance, reporting and data, and processes and systems – are in place.[67]

However, the United States Proxy Exchange provided their own strong views on proposals to penalize excessive risk taking that much of what happened during the Credit Crunch can be put down to good old fashioned abuse:

> In the midst of the most recent market crisis, Congress and other branches of our government didn't wait for hearings to embrace Wall Street's excuse that "excessive risk" was to blame. We believe this shifting of blame from abuse, where the blame correctly belongs, to excessive risk, where it does not, is forestalling appropriate legislative and regulatory initiatives that might prevent future market panics. We believe the current administration's proposal to form a systemic-risk regulator is, regretfully, misguided. What our economy needs is a systemic-abuse regulator. Excessive risk taking is one form of abuse, and it may be motivated by perverse incentive compensation schemes, but it is not the only one:
>
> - Putting low-income families into mortgages they cannot afford is "predatory lending." It is a form of abuse unrelated to "excessive risk taking."
> - Routinely falsifying those families' mortgage applications is to ensure they are approved is "fraud." It too is a form of abuse unrelated to "excessive risk taking."
> - Bundling those structured-to-fail mortgages into CDO's and giving them investment grade ratings is "deception." It too is a form of abuse unrelated to "excessive risk taking."
> - Parking the toxic CDO's in affiliated hedge funds and providing those hedge funds inflated valuations to hide the losses is "collusion." It too is a form of abuse unrelated to "excessive risk taking."
> - Foisting those hedge funds on unsuspecting institutional investors and charging them "2 and 20" for the privilege is "manipulative sales practices." It too is a form of abuse unrelated to 'excessive risk taking.[68]

The Financial Reporting Council expressed concern over the way inconsistent terminology meant that different words were used to explain the same thing. They gave the example of over 30 different expressions of probability thresholds embedded in the IFRS literature, ranging from 'remote' to 'probable' to 'virtually certain' including the following terms:

- unavoidable
- virtually certain

- no realistic alternative
- substantially
- highly
- reasonably certain
- majority
- major
- most
- principally
- expects
- more likely than not
- probable
- normally
- likely
- commonly
- may
- possible
- rarely
- highly unlikely
- highly abnormal
- extremely unlikely
- extremely rare.[69]

The search for more effective risk management is now the norm in all but the smallest of organizations. External assessment agencies are now seeking better ways of assessing entities as is clear from an account of the way Standard & Poor undertake corporate analysis:

> GAMMA (Governance, Accountability, Management Metrics & Analysis) is Standard & Poor's new emerging markets equity product, designed for equity investors in emerging markets and specifically focusing on non-financial risk assessment. Good corporate governance creates shareholder value and reduces risks for investment. Independent opinions on corporate governance, management, and accountability practices of individual companies are particularly valuable in emerging markets....Standard & Poor's has developed criteria and methodology for assessing corporate governance since 1998 and has been actively assessing companies' corporate governance practices since 2000. In 2007, the methodology of stand-alone governance analysis underwent a major overhaul to strengthen the risk focus of the analysis based on the group's experience assigning governance scores. GAMMA analysis focuses on a number of risks that vary in probability and expected impact on shareholder value. Accordingly, our analysis seeks to determine the most vulnerable areas prompt to potential losses in value attributable to governance deficiencies. Recent developments in the international financial markets emphasize the relevance of enterprise risk management and the strategic process to governance quality. GAMMA methodology incorporates two new elements, addressing these areas of investor concern. It also promotes the culture of risk management and long-term strategic thinking among companies.[70]

The emergence of risk management as a powerful way of enhancing corporate performance means that we must start with strategic risk before we drill down into the various specific risks that face most management teams, as made clear by the Institute of Corporate Directors:

> While there is some debate about the board's role in strategy, there is no question of the board's responsibility to oversee risk. The two are inseparable. Risk management must encompass the risk inherent in the strategy or it is missing probably the largest risks of all. However, strategic risk management well executed adds value to the strategy, not only by reducing downside risk, but also by increasing the potential of upside opportunities.[71]

One major issue that is now emerging as an obstacle to effective risk management is the role of the audit committee and the fact that many organizations' assigners assign the majority of risk-related tasks to their audit committees, which can lead to a dangerous overload. The National Association of Corporate Directors has warned of this heavy burden on audit committees:

> The combination of risk oversight with other mandated responsibilities can be overwhelming. While risk events may ultimately find their way to the audit committee because of its responsibility for oversight of financial reporting, other committees as well as the full board should participate. Many risks (e.g., technological obsolescence, product quality, mergers/acquisitions, and sales practices) lie outside the audit committee and require other committees – if not the full board – to oversee. The full board may want to consider assigning oversight of risks to certain committees to help ensure adequate coverage. Currently, only one out of four boards uses the full board for their risk oversight, while an even slimmer 6 percent use a risk committee. Boards can benefit from weighing the pros and cons of these different oversight paradigms for their companies. Whether directors use the full board or committees, they must devote greater attention to the primary duty of vigorously probing and testing management's assumptions. Risk oversight is a full board responsibility. However, certain elements can be best handled at the committee level with the governance committee coordinating those assignments. Similarly, the board must ask management: "Who is the owner of each risk area?" Management should identify the personnel responsible to manage and mitigate specific risk areas. Assignment of senior level responsibility will improve the accountability and reliability of information coming from management.[72]

The National Association of Corporate Directors goes on to call for improved risk identification procedures and mentions the importance of internal auditors as a crucial function in this respect:

> Management has the primary responsibility for the identification of risk. In a recent NACD member poll, a large majority (76.3 percent) of directors indicated that management provides directors with the information they need to effectively execute their risk governance role. However, those same directors said that two of the top challenges in providing risk oversight are: 1) management's capacity to define and explain the organization's risk management structure and process, and 2) the organization's capacity to identify and assess risks. Directors are increasingly concerned about risk oversight and will become more actively engaged in supporting the company's efforts to manage risk. Boards can prepare by selecting directors who have broad experience as well as industry expertise. Directors must then utilize their internal and external sources of information. Internal auditors can serve a crucial function because they are often on the front lines in identifying the likelihood of risk events and can raise these issues to the board level. Externally, outside sources of information, such as consultants or even D&O insurance agents, can provide new insight beyond what management supplies. Directors should also be aware that in some of the recent corporate meltdowns, the high-risk behaviors occurred in relatively small pockets of large companies. Therefore, understanding smaller high-risk operations is an important element. These changes in board behavior will likely improve the overall effectiveness of identifying risks for the company.[73]

The Walker Review highlighted the basic role of the board in governing the risk-management process:

> The focus in this Review is on how governance of risk by the boards of BOFIs can be made more effective alongside such enhanced regulation and supervision. In the past, some boards may have seen risk oversight as a compliance function essentially designed to meet regulatory capital requirements at minimum constraint on leveraged utilisation of the balance sheet. There has probably also been an element of "disclosure fatigue", leading to some sense that a large part of the board's obligations in respect of risk in the entity can be discharged through full disclosures. Such attitudes should have no place in the proper governance of risk in future. In essence, the obligation of the board in respect of risk should be to ensure that risks are promptly identified and assessed; that risks are properly controlled; and that strategy is informed by and aligned with the board's risk appetite.[74]

Walker went on to describe the key principles underpinning a board risk committee report that he felt should be included in the annual report and accounts, as follows:

- ***Strategic Focus*** – the report should seek to put the firm's agreed strategy into a risk management context, this should include information on the inherent risks to which the strategy exposes the firm.
- ***Forward Looking*** – the report should provide information to the reader that indicates the impact of potential risks facing the business – it should be clear for example whether a firm would be materially exposed to a fall in property prices for example. If the firm carries out stress testing, the report should reveal high level information on this stress testing programme. This should include the nature of the stresses, the most significant stresses and how the significance has changed during the reporting period.
- ***Risk Management Practices*** – the report should provide a brief description of how risk is managed in the business, ideally using examples of material risks that arose in the previous reporting period. In particular this should focus on the role of the Committee in the management of that risk. In addition the report should provide a brief statement on the number of meetings in the reporting period, an attendance record and whether any votes were taken. The report should cover the key responsibilities of the board risk committee and whether these have changed in the reporting period. Finally the report should briefly record the key areas that the committee has considered in the reporting period.[75]

Another ongoing debate revolves around the distinction between conformance and performance. So regulations that say each enterprise should have a sound risk-management process exist to ensure there is a process and it is adhered to because the rules say so or that they exist to ensure the enterprise can create and protect its core business. Deloitte makes clear their position in this debate:

> At many organizations, risk governance and value creation are viewed as opposed or even as mutually exclusive, when in fact they are inseparable. Every decision, activity, and initiative that aims to create or protect value involves some degree of risk. Hence, effective risk governance calls for Risk Intelligent governance – an approach that seeks not to discourage appropriate risk-taking, but to embed appropriate risk management procedures into all of an enterprise's business pursuits.[76]

The British standard on risk management has established several important principles that cover an organization's overall approach:

i) **Risk management should be tailored**
The organization should have an approach to risk management which is proportionate and scaled to address the context.

ii) **Risk management should take into account organizational culture, human factors and behaviour**
The organization's risk management processes should take into account the capabilities, perceptions and intentions of the people in the organization and other relevant stakeholders who might facilitate or hinder attainment of the organization's objectives.

iii) **Risk management should be systematic and structured**
The approach to risk management should be consistently applied within the organization. this helps ensure that the outputs of the **risk management process** are both reliable and comparable, and gives managers increased confidence to make effective decisions.

iv) **Risk management should operate under a common language**
The organization should apply a common language when identifying, assessing and responding to risks, and maintaining its risk management framework.

v) **Risk management should be based on the best available information**
The inputs to the risk management process should be based on relevant information sources, such as reported experience, subject knowledge, expert judgment and projected forecasts. Managers should be aware of any limitations to the data or divergence of opinion among experts.

vi) **Risk management should explicitly address uncertainty**
The organization should use risk management to help clarify the nature of uncertainty, how this might affect decisions and how it might be treated.

vii) **Risk management should be part of decision making**
Risk management should support informed decision making by helping to understand risks. this aids the organization in making a decision concerning its **risk appetite** and ability to manage the risks effectively.

viii) **Risk management should protect everything of value**
Risk management should contribute to the achievement of objectives and maximize benefits through integration with management processes, taking account of legislative, regulatory and compliance requirements.

ix) **Risk management should be transparent and inclusive**
The organization's managers should ensure that all stakeholders are identified, informed and appropriately involved in **risk identification**, assessment and response.

x) **Risk management should be dynamic, iterative and responsive to change**
The organization should ensure its risk management continually identifies and responds to changes affecting its operating environment (context).

xi) **Review of the principles**
The way in which the risk management principles are applied should be subject to regular review to reflect changes in the organization's nature and context.[77]

To close this section on new developments, we have a look at the perennial problem of how to classify risk. Help is one hand from Ernst and Young who have described one useful way of categorizing risk:

Financial risks

- Accounting and reporting (e.g., accounting, reporting, internal controls)
- Market (e.g., interest rate, currency)
- Liquidity and credit (e.g., cash management, hedging)

- Tax (e.g., tax strategy and planning, indirect taxes, transfer pricing)
- Capital structure (e.g., debt, equity, options)

Strategic risks

- Planning and resource allocation (e.g., organization structure, strategy, budgeting)
- Communications and investor relations (e.g., media, investor and employee communications)
- Major initiatives and capital programs (e.g., vision, planning, execution, monitoring)
- Competitive market dynamics (e.g., competitive pricing)
- Mergers, acquisitions and divestitures (e.g., valuation, due diligence, integration)
- Macro-market dynamics (e.g., economic, social, political)

Compliance risks

- Governance (e.g., board, tone at the top)
- Regulatory (e.g., labor, safety, trade/customs)
- Legal (e.g., contracts, intellectual property)
- Code of conduct (e.g., ethics, fraud)

Operational risks

- Information technology (e.g., IT management, security, availability)
- Physical assets (e.g., real estate; property, plant and equipment)
- Sales and marketing (e.g., advertising, pricing, customer support)
- People (e.g., recruiting, retention, development)
- Research and development (e.g., market research, product design and development, product testing)
- Supply chain (e.g., planning, inventory, distribution)
- Hazards (e.g., natural events, terrorist acts)[78]

Summary and Conclusions

Risk management is not really a management fad. It provides a platform for corporate governance by giving comfort to shareholders and other stakeholders that the risks to their investment (or services) are understood by their representatives, the board and systematically addressed by the management. True risk management is about changing the culture of the organization to get people to embrace their responsibilities knowing that this tool will help them get around problems and drive the business forward in a considered manner. Peter Bernstein raises some interesting issues for those that make risk assessment a numbers game:

> We cannot quantify the future, because it is unknown, but we have learnt how to use numbers to scrutinise what happened in the past. But to what degree should we rely on the patterns of the past to tell us what the future will be like? Which matters more when facing risk, the facts as we see them or our subjective belief in what lies hidden in the void of time? Is risk management a science or an art?[79]

David McNamee and Georges Selim's work on changing the internal auditor's paradigm describes how internal audit's new paradigm from internal control to business risk means a move away from being reactive and after the fact towards a co-active, real-time participant in strategic planning [80]

> The internal auditor's push into a consulting role at board level is a major step that takes a great deal of courage, and a lifting of the veil of audit independence to make risk management work properly. All the same, risk management does not mean perfection, and an empathy with the people who work for an organization means understanding is often better than blame for any real progress to be made: The driver of a train which crashed killing seven people and injuring 150 broke down at a public inquiry in the disaster yesterday. He was led away, weeping, after admitting he was partly to blame for the accident at Southall, West London in September 1997, 'We are all human,' he said. 'I made a mistake.'[81]

The development of risk management has a driving force that shows no sign of slowing down. In terms of the response from government to the whole concept of identifying risk, managing risk and telling the public about the implications, this issue has resumed a high profile. The Government's (Cabinet Office – Strategy Unit) Report on Risk: Improving Government's Capability to Handle Risk and Uncertainty (Nov 2002) contained six wide-ranging recommendations:

1. Handling risk should be firmly embedded in government's policy making, planning and delivery.
2. Government's capacity to handle strategic risks should be enhanced.
3. Risk handling should be supported by good practice, guidance and skills development.
4. Departments and agencies should make earning and maintaining public trust a priority when dealing with risks to the public.
5. Ministers and senior officials should take a clear lead in improving risk handling.
6. The quality of government risk management should be improved through a two-year programme of change, linked to the Spending Review timetable, and clearly set in the context of public sector reform.[82]

Our final word comes from a speech by James Lam: 'Let me leave you with a final thought. Over the longer term, the only alternative to risk management is crisis management, and crisis management is much more embarrassing, expensive and time-consuming.'[83]

Chapter 3: Assignment Questions

Having worked through the chapter, the following questions may be attempted (see Appendix A). Note that the question number relates to the section of the chapter that contains the relevant material.

1. Describe the concept of risk and suggest ways that this concept can be applied to business practice.
2. Discuss the implications of high levels of unmitigated risk in terms of both threats to the business and missed opportunities.
3. Describe the risk-management cycle and discuss each of the main stages.
4. Discuss the view that high levels of business risk may be addressed through a variety of methods.
5. Explain the concept of risk registers and how they are affected by the adopted risk appetite.
6. Describe the contents of a corporate risk policy and explain the role of a CRO in implementing this policy.
7. Explain what is meant by 'enterprise-wide risk management' and describe the way that this concept may be developed for an organization.

8. Explain how control self-assessment can be used to implement risk management.
9. Explain the steps that an organization may take to embed risk management into the business and the way people behave at work.
10. Prepare a presentation to the internal audit management team on the role of internal audit in the organization's efforts to establish and validate business risk management.

Chapter 3: Multi-choice Questions

3.1 Insert the missing words:
David McNamee and Georges Selim argue that: The implications of this ..... are enormous. It turns the focus of the audit away from the past and present and toward the present and future. Focusing on controls over transactions buried the internal auditor in the details of the past, limiting the value from any information derived.
   a. new dimension
   b. paradigm shift
   c. risk shift
   d. new focus

3.2 Insert the missing word:
The point is that success in business and the public sector is intimately tied into the act of risk taking. Risk arises from ..... and controls are based on reducing this uncertainty where both possible and necessary.
   a. hazards
   b. chance
   c. certainty
   d. uncertainty

3.3 Which is the most appropriate statement?
   a. Risk has no real form unless we relate it to our own direction, that is, what we are trying to achieve.
   b. Risk has no real form unless we relate it to known hazards, that is, what we are trying to achieve.
   c. Risk has no real form unless we relate it to our own direction, that is, what we are trying to avoid.
   d. Risk has no real form unless we relate it to our own direction, that is, what we are certain to achieve.

3.4 Which is the most appropriate statement?
   a. The other concept that needs to be considered is that risk, in the context of achieving objectives has both an upside and downside. In our model we call these right and wrong directions.
   b. The other concept that needs to be considered is that risk, in the context of achieving objectives has both an upside and downside. In our model we call these threats and negatives.
   c. The other concept that needs to be considered is that risk, in the context of achieving objectives has both an upside and downside. In our model we call these threats and opportunities.
   d. The other concept that needs to be considered is that risk, in the context of achieving objectives has both an upside and downside. In our model we call these risk averse and risk taking.

3.5 Which is the most appropriate statement?

a. This is why risk management is not really about building bunkers around the team to protect them from the outside world. It is more about staying within familiar areas and knowing when and where to take risks.
b. This is why risk management is not really about building bunkers around the team to protect them from the outside world. It is more about moving outside of familiar areas and knowing when and where to take risks.
c. This is why risk management is not really about building bunkers around the team to protect them from the outside world. It is more about avoiding familiar areas and knowing when and where to take risks.
d. This is why risk management is not really about building bunkers around the team to protect them from the outside world. It is more about moving outside of familiar areas and accepting all risks.

3.6 Which is the most appropriate statement?

a. The next point to address is the basic two dimensions of measuring risk. That is, as well as defining the nature of the risk, we need also to think about the extent to which the risk has already materialized.
b. The next point to address is the basic two dimensions of measuring risk. That is, as well as defining the impact of the risk, we need also to think about the extent to which the risk is likely to materialize.
c. The next point to address is the basic two dimensions of measuring risk. That is, as well as defining the impact of the risk, we need also to think about the extent to which the risk has already materialized.
d. The next point to address is the basic two dimensions of measuring risk. That is, as well as defining the certainty of the risk, we need also to think about the extent to which the risk is likely to materialize.

3.7 Insert the missing words:

Before we can delve into risk management we need to make a further point. That is, that risk management is mainly dependant on establishing the . . . . . , or the person most responsible for taking action in response to a defined risk, or type of risk, or risk that affects a particular process or project.

a. risk owner
b. project manager
c. target manager
d. supervisor

3.8 Which is the odd one out?

The risk-management cycle includes the following stages:

a. identification
b. assessment
c. migration
d. management
e. review

3.9 What is abc?

The subject of **abc** has a very interesting past. Project managers have used them for a long time as they assess risks at an early stage in a large project and enter the details in a formal record that is inspected by the sponsors. The insurance industry again is well used to documenting assumptions about risk and using this to form judgements on where to offer insurance cover and what aspects of an operation are included in this cover. More recently,

they have come to the fore as an important part of general business risk management. **abc** acts as a vehicle for capturing all the assessment and decisions made in respect of identified risks. Moreover, the **abc** may form part of the assurance process where they can be used as evidence of risk containment activity that supports the SIC.

3.10 Insert the missing words:

The majority of risk-management guides refer to tolerance, acceptance, appetite and other such measures of what we have called unmanaged .....

a. negative risk
b. key issues
c. marginal risk
d. residual risk

3.11 Which is the most appropriate statement?

a. Much confusion results from mixing gross and net risk. Risk before we have put in measures to deal with it, is net, or what we have called inherent risk. Risk that has been contained so far as is practicable is gross, or what we have called residual risk.
b. Much confusion results from mixing gross and net risk. Risk before we have put in measures to deal with it, is gross, or what we have called inherent risk. Risk that has been contained so far as is practicable is net, or what we have called residual risk.
c. Much confusion results from mixing gross and net risk. Risk before we have put in measures to deal with it is gross, or what we have called residual risk. Risk that has been contained so far as is practicable is net, or what we have called inherent risk.
d. Much confusion results from mixing gross and net risk. Risk after we have put in measures to deal with it is gross, or what we have called inherent risk. Risk that has been contained so far as is practicable is net, or what we have called residual risk.

3.12 Which is the most appropriate statement?

a. The result of people buy-in is that we can get closer to a risk managed culture where people around the organization take responsibility for isolating risks and making sure they provide a criteria for making key decisions.
b. The result of people buy-in is that we can get closer to a risk averse culture where people around the organization take responsibility for isolating risks and making sure they provide a criteria for making key decisions.
c. The result of people buy-in is that we can get closer to a risk managed culture where people around the organization take responsibility for isolating risks and making sure they provide a criteria for avoiding all risks.
d. The result of people buy-in is that we can get closer to a blame culture where people around the organization take responsibility for isolating risks and making sure they provide criteria for making key decisions.

3.13 Which is the odd one out?

There is a useful model that can be applied to promoting successful seminars, by building several considerations into the planning phase of the communications project (via the seminars):

a. understand nature of risk
b. appreciate our risk policy
c. accept the need for control self-assessment
d. appreciate links to corporate governance
e. understand that employees should not take risks
f. look forward to the risk workshops.

3.14 Insert the missing words:
In future, new recruits will arrive at an organization with the key question ..... and feel quite comfortable working with whatever process has been developed and employed.
a. 'how do you avoid risk here?'
b. 'how do you accept risk here?'
c. 'how do you manage risk here?'
d. 'how do you tolerate risk here?'

3.15 Insert an appropriate missing word:
..... management is another topical risk area and this tends to be the culmination of the way an organization has managed all the other risks to its business.
a. Performance
b. Reputation
c. Regulation
d. Strategic

3.16 Which is the most appropriate statement?
a. Quite often, communications strategies revolve around the subtle difference between warning people and protecting people.
b. Quite often, communications strategies revolve around the subtle difference between assisting people and working with people.
c. Quite often, communications strategies revolve around the subtle difference between warning people and scaring people.
d. Quite often, communications strategies revolve around the subtle difference between frightening people and scaring people.

3.17 Which is the odd one out:
The Department of Health has established a guide to Communicating About Risk to Public Health which suggests that:
a. messages are usually judged first by whether their source is trusted;
b. intentional communication is often only a minor part of the message actually conveyed;
c. responses to messages depend not only on content but also on the manner of delivery, especially emotional tone;
d. all messages are accepted if they seem plausible;
e. experts no longer command automatic trust, no matter how genuine their expertise, trust is generally fostered by openness, both in the sense of avoiding secrecy and in being ready to listen.

3.18 Insert an appropriate missing phrase:
Proponents of ..... are convinced that the only way to get risk management into the heart and minds of the organization is to get everyone involved in a participative manner.
a. performance management
b. CRSA
c. downsizing
d. auditing

3.19 Insert the missing phrase:
The need to balance independence and the assurance and consulting roles of internal audit is a growing feature of the new look internal auditor. The value add equation means we cannot ignore the need to .....
a. assure as well as review

b. help as well as facilitate
c. help as well as review
d. help and not review

3.20 Insert the missing phrase:
Risk management is not really a management fad. It provides a platform for .... by giving comfort to shareholders and other stakeholders that the risks to their investment (or services) are understood by their representatives, the board and systematically addressed by the management.
a. accountability
b. success
c. good performance
d. corporate governance

3.21 Which is the most appropriate statement?
a. The internal auditor's push into an assurance role at board level is a major step that takes a great deal of courage, and a lifting of the veil of audit independence to help make risk management work properly.
b. The internal auditor's push into a consulting role at board level is a major step that takes a great deal of courage, and a lifting of the veil of audit independence to help make risk management work properly.
c. The internal auditor's push into a consulting role at board level is a major step that takes a great deal of courage, and a lifting of the veil of audit independence to help make audit work properly.
d. The internal auditor's push into an assurance role at board level is a major step that takes a great deal of courage, and a lifting of the veil of audit independence to help make audit work properly.

3.22 What is abc?
Over the longer term, the only alternative to risk management is abc, and abc is much more embarrassing, expensive and time-consuming.
a. crisis management
b. strategic management
c. contingency management
d. continuity management

References

1. McNamee David and Selim Georges, 'IIA Research Foundation, 'Risk management: changing the internal auditor's paradigm", *Internal Auditing*, Dec. 1998, pp. 6–9.
2. 'Think risk and survive'. *Internal Auditing*, Nov. 1998, p. 34, ICAEW Moorgate Internal Audit Lecture.
3. Chapman Christy. 'Raising the bar'. *Internal Auditor*, April 2001, p. 56.
4. Bernstein Peter L. (1996) *Against the Gods*, New York: John Wiley and Sons Inc., p. 8.
5. Bernstein Peter L. (1996) *Against the Gods*, New York: John Wiley and Sons Inc., p. 3.
6. *Daily Mail*, 2 Oct. 1996, 'Financial wizard's reward for risk-taking'.
7. *Daily Mail*, 10 Dec. 1996, 'Explorer goes up the pole at Boots'.
8. *Daily Mail*, 18 Aug. 1996.
9. *South London Press*, Friday 21 Nov. 1997, p. 23, 'Probe into tower block blast', Perry Andrea.
10. *South London Press*, Friday 12 July 1996, p. 31, 'Bosses spared axe over cash boob', Gardner Andy.
11. *Daily Mail*, 28 Jan. 1998, p. 17, 'Anger of BSE families over inquiry with no one to blame', Poulter Sean.
12. *Daily Mail*, 1 Oct. 1997, p. 33, 'Trainee doctors "put lives at risk".

13. Bernstein Peter, L. (1996) *Against the Gods*, New York: John Wiley and Sons Inc., p. 20.
14. Shapiro Eileen, C. 1996, *Fad Surfing in the Boardroom*, Capstone Publishing Ltd.
15. Bernstein Peter, L. (1996) *Against the Gods*, New York: John Wiley and Sons Inc., p. 337.
16. Tone at the Top, Published by the IIA, issue 11 Sep. 2001, 'Risk or opportunity – the choice is yours', para. 20.
17. BS6079-3:2000 Project Management Part 3 – Guide to the Management of Business Risk, 2000.
18. *Daily Mail*, Thursday 12 Sep 1996, p. 3, 'Pilot who found he hated heights – at 33,000 ft'.
19. Top Risks in the Private Sector (1999), Deloitte & Touche Survey of Significant Risks.
20. Brown Steve 'NHS get intensive on risk', *Accountancy Age*, 25 Nov. 1999.
21. British Standards Institute, 'Risk management 21 21 code of practice', BS 31100:2008, p. 20–21, BSi 2008, iCS 03.100.01.
22. Bernstein Peter, L. (1996) *Against the Gods*, New York: John Wiley and Sons Inc., p. 197.
23. Bernstein Peter, L. (1996) *Against the Gods*, New York: John Wiley and Sons Inc., p. 335.
24. Bernstein Peter, L. (1996) *Against the Gods*, New York: John Wiley and Sons Inc., p. 263.
25. Flesher Dale (1996) *Internal Auditing: A One-Semester Cours*e, Florida: The Institute of Internal Auditors, p. 122.
26. *Daily Mail*, Friday 7 Dec. 2001, p. 81, Sunderland Ruth.
27. *Mail on Sunday*, 6 April 1997, 'Stable lad defies the bombers'.
28. *Mail on Sunday*, Night and Day, p. 18, 'Most dangerous jobs'.
29. *Evening Standard*, 11 May 2000, 'Paddington: rails chief threw out £5m safety plan'.
30. *Daily Mail*, 2 Nov. 1999.
31. Orsini Basil, 'Mature risk management: risk management diagnostic tool'. *Internal Auditing*, Aug. 2002, pp. 66–67.
32. ICAEW Website, www.icaew.co.uk, Thursday 8 Sept. 2002.
33. NAO, 'Supporting innovation: managing risk in government departments, 26 July 2000.
34. British Standards Institute, 'Risk management – Code of practice', BS 31100:2008, 2008, p. 12, BSi 2008, iCS 03.100.01
35. Orsini Basil, 'Mature risk management: risk management diagnostic tool', *Internal Auditing*, Aug. 2002, pp. 66–67.
36. Hill Gordon 'Managed risk'. *Internal Auditor*, April 1999, p. 14.
37. Department for Education and Skills, *Statement on the Management of Risks Affecting the Public*, Risk Assessment for Schools.
38. Hala Nancy 'Unlock the potential'. *Internal Auditing*, Oct. 2002, pp. 30–35.
39. Orsini Basil, 'Mature risk management: risk management diagnostic tool'. *Internal Auditing*, Aug. 2002, pp. 66–67.
40. Piper Arthur 'Escaping Babel'. *Internal Auditing and Business Risk*, May 2002, pp. 16–19.
41. 'Risk management in the public services', CIPFA, p. 18, para. 1.2.
42. British Standards Institute, 'Risk management – Code of practice', BS 31100:2008, pp. 7–8, BSi 2008, iCS 03.100.01.
43. Chapman Christy, 'The big picture'. *Internal Auditor*, June 2001, pp. 30–37.
44. Chapman Christy 'The big picture'.*Internal Auditor*, June 2001, p. 30.
45. 'Risk management in the public services', CIPFA, 2001, p. 18, para. 1.4.
46. Hodge Neil 'Called to account'. *Internal Auditing and Business Risk*, Dec. 2001, pp. 12–16.
47. British Telecom (www.bt.com), 2005.
48. Steckel Colette 'Crisis management'. *Accounting and Business*, May 2001, p. 13.
49. Chambers Andrew 'Is reputation all?' *Internal Auditing*, Sept. 1999, p. 36, ICAEW Audit Faculty Moorgate Lecture.
50. Livesey Alan 'The spreadsheet is dead! Long live the spreadsheet'. *Internal Auditing and Business Risk*, March 2001, p. 24.
51. Bennett Peter (1999) 'Understanding responses to risk: some basic findings' in *Risk Communication and Public Health*, Bennet Peter and Calman Kenneth (eds), Oxford University Press.
52. Department of Health, 'Communicating about risk to public health', 1998.
53. HMT Risk Management Framework, Feb. 2001.
54. ICAEW Website, Thursday 13 June 2002, Wyman Peter, President of the Institute (www.icaew.co.uk).
55. Makosz Paul, Sentinel, No. 1, Jan. 1997, Published by the IIA and the IIA Control Self-Assessment Center.

56. Hill Gordon 'Embedding Turnbull, achieving a managed risk culture'. *Internal Auditing and Risk Management*, p. 30.
57. LCD Risk Management Framework 2002, para. 4 Communication (www.lcd.gov.uk).
58. Atwater Geoffrey 'Culture of assurance'. *Internal Auditor*, pp. 56–59.
59. Bolton Gill 'Organisational risk management'. *Internal Auditing*, Oct. 1999, p. 6.
60. Professional Briefing Note Thirteen, Managing Risk, IIA.UK, Internal Audit's Role In Managing Risk, 1998.
61. 'Getting to grips with ERM'. *Internal Auditing and Business Risk*, Aug. 2002, p. 11.
62. Maynard Gregg R. 'Embracing risk'. *Internal Auditor*, Feb. 1999, p. 24.
63. HM Treasury Guide, Strategic Risk Management, 2004.
64. Wynne Andy 'Risk management comes of age'. *Accounting and Business*, 1999, p. 91.
65. 'IIA.UK&Ireland, Position statement – responsibilities on risk'. *Internal Auditing and Business Risk*, July 2002, p. 32.
66. British Standards Institute, 'Risk management – Code of practice', BS 31100:2008, p. 12, BSi 2008, iCS 03.100.01.
67. 'Risk management is it permanently broken?'. An Investment Management Perspective, p. 3, 2009. KPMG LLP, A U.S. limited liability Partnership.
68. 'Comments of the United States Proxy Exchange', September 15, 2009, pp. 3–4, Re: File No. S7-13-09, Proxy Disclosure and Solicitation Enhancements.
69. Financial Reporting Council, Louder Than Words 2009, (Principles and actions for making corporate reports less complex and more relevant), p. 36.
70. Standard & Poor. Standard & Poor's, a Division of The McGraw-Hill Companies, Inc. 2008, The McGraw-Hill Companies, p. 4.
71. *Institute of Corporate Directors, Issue 143, April 2009, p. 13, Hugh Goldie, Ken Smith and Peter Stephenson.*
72. WHITE PAPERS: SERIES I pp. 8–10, *Risk Oversight Transparency Strategy Executive Compensation*, 2009, National Association of Corporate Directors.
73. WHITE PAPERS: SERIES I, pp. 8–10, *Risk Oversight Transparency Strategy Executive Compensation*, 2009, National Association of Corporate Directors.
74. The Walker Review, A review of corporate governance in UK banks and other financial industry entities, para 6.3, 16 July 2009.
75. The Walker Review, A review of corporate governance in UK banks and other financial industry entities, annex 10, 16 July 2009.
76. Risk Intelligent governance, A practical guide for boards, p. 2, Risk Intelligence Series, Issue No. 16, 2009, Deloitte Development LLC, Member of Deloitte Touche Tohmatsu.
77. British Standards Institute, 'Risk management – Code of practice', BS 31100:2008, pp. 3–4, BSi 2008, iCS 03.100.01.
78. 'The future of risk: protecting and enabling performance', p. 3, Ernst and Young, 2009.
79. Bernstein Peter, L. (1996) *Against the Gods*, New York: John Wiley and Sons Inc., p. 6.
80. McNamee David and Selim Georges, IIA Research Foundation. 'Risk management: changing the internal auditor's paradigm'. *Internal Auditing*, Dec. 1998, p. 135.
81. *Daily Mail*, 29 Sept. 1999, 'Weeping death crash railman says: I made a mistake'.
82. Cabinet Office – Strategy Unit Report on Risk: Improving Government's Capability to Handle Risk and Uncertainty, Nov. 2002.
83. James Lam, Speech at the IQPC Enterprise Risk Management Conference, 25 March 1999.

Chapter 4

INTERNAL CONTROLS

Introduction

We have so far referred to corporate governance and risk management; internal control forms the third component of this stool. Good governance is dependent on a management that understands the risks it faces and is able to keep control of the business. *Brink's Modern Internal Auditing* suggests that internal control is the most important and fundamental concept that an internal auditor must understand.[1] Note that all references to IIA definitions, code of ethics, IIA attribute and performance standards, practice advisories and practice guides relate to the IPPF prepared by the IIA in 2009. This chapter covers the following areas:

4.1 Why Controls?
4.2 Control Framework – COSO
4.3 Control Framework – CoCo
4.4 Other Control Models
4.5 Links to Risk Management
4.6 Control Mechanisms
4.7 Importance of Procedures
4.8 Integrating Controls
4.9 The Fallacy of Perfection
4.10 Internal Control Awareness Training
4.11 New Developments
Summary and Conclusions
Assignments and Multi-choice Questions

We will build a model of control that is used to capture most of the key features of a sound system of internal control. Much is dependent on the control environment and there is a view that, if an organisation can get this right, the rest will tend to follow. The trend towards risk management as the way forward for ensuring objectives are achieved does not mean that controls, as a fundamental aspect of risk management, are any less important. The control framework covers the risk management process and the use of tailored control mechanisms is a fundamental aspect of business life. We try to demonstrate why a good understanding of internal control is important in achieving sound corporate governance and Section 4.10 contains advice on delivering control awareness training for staff. Many risk workshops fail to provide insights into what control is about and why it is important and we hope to address this failing in this chapter.

4.1 Why Controls?

The Committee of Sponsoring Organizations (COSO) of the Treadway Commission (www.coso.org) have suggested that:

> Senior executives have long sought ways to better control the enterprises they run. Internal controls are put in place to keep the company on course toward profitability goals and achievement of its mission, and to minimize surprises along the way. They enable management to deal with rapidly changing economic and competitive environments, shifting customer demands and priorities, and restructuring for future growth. Internal controls promote efficiency, reduce risk of asset loss, and help ensure the reliability of financial statements and compliance with laws and regulations. Because internal control serves many important purposes, there are increasing calls for better internal control systems and report cards on them. Internal control is looked upon more and more as a solution to a variety of potential problems.

Where there are risks to the achievement of objectives, which mean failure is a strong possibility, controls have to be put in place to address these risks. If not, failure becomes likely. At the same time, controls cost money and they have to be worthwhile. A lot depends on the risk appetite and what is considered acceptable as opposed to unacceptable to the organisation and its stakeholders. A report from the NAO back in 1998 on losses of £32 million concluded that a lack of proper financial controls and accountancy procedures in the pre-privatization restructuring of Her Majesty's Stationery Office cost the government millions of pounds.[2] Poor controls lead to losses, scandals and failures, and damage the reputation of organisations in whatever sector they are from. Where risks are allowed to run wild and new ventures are undertaken without a means of controlling risk, there are likely to be problems. Internal control is nothing new, and back in 1949, the American Institute of Certified Public Accountants (AICPA) argued that internal control comprises the plan of the organisation and all the coordinate methods and measures adopted within a business to safeguard its assets, check the accuracy and reliability of its accounting data, promote operational efficiency and encourage adherence to prescribed managerial practices. Internal auditors throughout the ages have argued the cause for good controls and the regulators have appreciated the need for control. It has been said that there is no substitute for internal control. It is the responsibility of management and the reason for the existence of internal auditors.[3]

The control banner is being waved by many authorities and regulators. For example, the Securities and Exchange Commission (SEC) regulations require organisations to devise and maintain a system of internal accounting control. The Turnbull report (see Chapter 2) suggests that:

> A company's system of internal control has a key role in the management of risks that are significant to the fulfilment of its business objectives. A sound system of internal control contributes to safeguarding the shareholders' investment and the company's assets. (para. 10) Internal control . . . facilitates the effectiveness and efficiency of operations, helps ensure the reliability of internal and external reporting and assists compliance with laws and regulations. (para. 11)

while the United Kingdom's 2008 Combined Code makes clear the need for good controls.

C.2 Internal Control

Main Principle

The board should maintain a sound system of internal control to safeguard shareholders' investment and the company's assets.

Code Provision

C.2.1 The board should, at least annually, conduct a review of the effectiveness of the group's system of internal controls and should report to shareholders that they have done so. The review should cover all material controls, including financial, operational and compliance controls and risk management systems.[4]

The original King report (para 3.2.1) from South Africa continues this drive to keep controls on the board room agenda and reasons that a comprehensive system of control should be established by the board to ensure that risks are mitigated and that the company's objectives are attained. The control environment should also set the tone of the company and cover ethical values, management's philosophy and the competence of employees. Control is everything that is in place to move successfully from the present to the future. The IIA takes this wide view and states that control is:

> Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved.

One writer has highlighted the dynamics of controls by saying that the purpose of any control system is to attain or maintain a desired state or condition.[5] We can build on the view that control is about achieving objectives, dealing with risk and keeping things in balance by introducing our basic first model of control in Figure 4.1.



FIGURE 4.1 Internal control (1).

An organisation will set clear objectives and then assess the inherent risks to achieving these objectives. Before it can reach the black achievements box, there needs to be a control strategy put in place to provide a reasonable expectation of getting there. The control strategy will be derived from a wider risk management strategy, but having as a key component, focused and effective systems of internal control. Effective controls are measures that work and give a reasonable probability of ensuring that operations are successful and resources protected. Where these controls contain obvious loopholes, there is a chance that this will be exploited:

> A woman bank executive was jailed for four-and-a-half years yesterday for stealing £1.75 million from her employers. Ms x, who earned £55,000 a year at the Dunbar Bank took cash from the tills and walked out with it in her pockets. After her arrest, she told police: 'It was so simple and easy to do. It was easy to spend thousands of pounds during my lunch hour, which I did frequently.' . . . She also stole by making transfers to a third party and by writing cheques and falsifying the information on the stubs.[6]

The IIA is the professional body that has real expertise in the subject of organisational control. The IIA has described the control environment as:

> The attitude and actions of the board and management regarding the significance of control within the organization. The control environment provides the discipline and structure for the achievement of the primary objectives of the system of internal control. The control environment includes the following elements:
>
> - Integrity and ethical values.
> - Management's philosophy and operating style.
> - Organizational structure.
> - Assignment of authority and responsibility.
> - Human resource policies and practices.
> - Competence of personnel.

The system of internal control needs to be adequate and we can turn again to the IIA for an understanding of what adequacy means. The IIA suggests that adequacy is present if:

> Management has planned and organized (designed) in a manner that provides reasonable assurance that the organization's risks have been managed effectively and that the organization's goals and objectives will be achieved efficiently and economically.

Control is not only about installing a range of procedures to ensure staff can get from A to B; it is also a process. Again, we can turn to others for help in defining what this means, and a process has been defined as:

> The policies, procedures, and activities that are part of a control framework, designed to ensure that risks are contained within the risk tolerances established by the risk management process.

Viewing internal control as a dynamic concept that runs across an organisation as opposed to a series of basic procedures takes the topic to a higher level. Turnbull provides some background as to what makes up a sound system of internal control:

> An internal control system encompasses the policies, processes, tasks, behaviours and other aspects of a company that, taken together:
>
> - facilitate its effective and efficient operation by enabling it to respond appropriately to significant business, operational, financial, compliance and other risks to achieving the company's objectives. This includes the safeguarding of assets from inappropriate use or from loss and fraud, and ensuring that liabilities are identified and managed;
> - help ensure the quality of internal and external reporting. This requires the maintenance of proper records and processes that generate a flow of timely, relevant and reliable information from within and outside the organisation;
> - help ensure compliance with applicable laws and regulations, and also with internal policies with respect to the conduct of business. (para. 20)

Management's Responsibilities

Turnbull has made clear where control responsibility lies in an organisation:

> The board of directors is responsible for the company's system of internal control. It should set appropriate policies on internal control and seek regular assurance that will enable it to satisfy

> itself that the system is functioning effectively. The board must further ensure that the system of internal control is effective in managing risks in the manner which it has approved. (para. 16)

While the board sets overall direction, it is management who must implement good controls by considering the following.

Determine the need for controls Managers must be able to isolate a situation where there is a need for specific internal controls and respond appropriately. For example, when designing a new computer system, they must consider controls over both the development process and the resulting system at an early stage as part of their overall responsibility to promote the welfare of the organisation. The determination of need precedes the design stage as there is little point in resourcing a control routine that is not really required. Another good example of this principle is where a previously in-house service is contracted out to an external provider. Here the contract specification along with suitable contract management procedures constitute key controls over the contract where it is monitored and compliance checked. Management must consider the need for additional controls over and above the contract compliance issue. This may include a review of the database for, say, a debtors system where accounts that are left out may simply be ignored and so not collected. Checks over the completeness of this database may be required to protect the organisation where there would be no other way of knowing whether the database was being properly maintained. The decision on whether to install extra controls is obviously relevant here and this decision must be left to management. A simple story demonstrates how the need for controls may not always be recognized:

> In the space of 92 minutes Stephen Humphries brought Sussex Futures to its knees. The rogue city trader ran up losses of £750,000 on the London International Financial Futures Exchange, effectively betting other people's money against a change in US interest rates . . . Last week, a year later, he was imprisoned for three years and two months; Sussex Futures, having racked up debts of £2.3 m went into liquidation earlier this year. The story has 'Barings' stamped all over it, albeit not quite the same scale or the same length of time, but the principles are the same; one rogue trader, trying to conceal his position, failing to trade out of his unauthorised position, then fleeing the crime scene.[7]

Design suitable controls Once the need for controls has been defined, management must then establish suitable means to install them. This is not a simple process that relies solely on doing what was done in the past. It involves much more, including a formal process of assessing relative risks and seeking to guard against the types of problems that might arise if controls are not firmly in place. We have already outlined the criteria that should be considered when devising controls, and these and much more should be taken on board in the design process. Managers know their staff, work environment and type of culture they operate within better than anyone else, which makes them well placed for this task. Consultants, auditors, project teams and other sources of advice may be employed in the search for improved control, but notwithstanding this, responsibility still lies with the managers themselves.

Implement these controls Managers are then duty bound to ensure that the control processes are carefully implemented. This entails, at a minimum, the provision of suitable guidance on how they should be used, ideally in written format and a mechanism by which staff can be coached in the application of the underlying actions. We may care to move back a step and suggest that managers have to think about the basic skills necessary to effect these controls and whether they are employing the right calibre of staff in this respect. Remember it is the responsibility of

management to deem that defined posts attract certain minimum qualifications and experience. If these are not asked for, then there is no point then blaming staff for poor performance. It is generally the managers' fault that their subordinates are not able to discharge the requirements of their post. Training and development are the other techniques that seek to support basic performance standards. This must be fully applied in the pursuit of success in line with the control arrangements that underpin this search.

Check that these controls are being applied correctly Management and not internal audit is responsible for ensuring that control mechanisms are not being bypassed but are fully applied as they were originally intended. One cannot wait for the auditors for information on how controls are working as this defeats this important principle. Management should seek to set control as a highly regarded discipline that deserves the respect of all staff and not an unnecessary set of rules that impair performance. All these things lead to an environment where control is fostered and publicized, again leading to the chance of greater compliance. It therefore becomes more and more difficult for managers to shrug their shoulders and declare that poor control is caused by junior staff and not them. Once we have arrived at this acceptance, we have great scope for a well-controlled organisation.

Maintain and update the controls This feature is also important in that securing control is a continuous task that should be at the forefront of management concerns. The need to define control implications must be revisited as we reinforce the view that management must acknowledge this issue in a vigorous way. This includes the need to discard outdated control wherever necessary so as to avoid the unmanageable situation where controls are perceived as patchy, with some being applied while others have fallen into disuse. So as to avoid excessive debate on the question of updating control, we can merely suggest that up-to-date procedures can be a life or death issue as one newspaper headline reads:

> Hundreds killed by doctors relying on outdated manuals. (*Sunday Times*, 5 February 1995)

Inclusion of the above noted matters within any appraisal scheme that seeks to judge management's performance We would expect management to consider the application of controls as part of management skills and training. Furthermore, if this were built firmly into employee performance appraisal mechanisms, then managers would be in the enviable position whereby they receive suggestions from their staff on how to better effect good control over the resources under their command.

Internal Audit's Role

The internal auditor has to be concerned about the state of control in the organisation. The pace has been set by the IIA whose Performance Standard 2130 goes straight to the point: 'The internal audit activity must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.' The auditors' role regarding systems of internal control is distinguished from management's in that it covers:

- assessing those areas that are most at risk in terms of the key control objectives that we have already mentioned (i.e. MIS, compliance, safeguarding assets and VFM);

- defining and undertaking a programme for reviewing these high profile systems that attract the most risk;
- reviewing each of these systems by examining and evaluating their associated systems of internal control to determine the extent to which the five key control objectives are being met;
- advising management whether or not controls are operating adequately and effectively so as to promote the achievement of the system's/control objectives;
- recommending any necessary improvements to strengthen controls where appropriate, while making clear the risks involved for failing to effect these recommended changes;
- following up audit work so as to discover whether management has actioned agreed audit recommendations.

The Basel Committee on Banking Supervision has prepared a Framework for Internal Control Systems in Banking Organisations (September 1998), which talks about the need for internal audit and states that:

> there should be an effective and comprehensive internal audit of the internal control system carried out by operationally independent, appropriately trained and competent staff. The internal audit function, as part of the monitoring of the system of internal controls, should report directly to the board of directors or its audit committee, and to senior management. The internal audit function is an important part of the ongoing monitoring of the system of internal controls because it provides an independent assessment of the adequacy of, and compliance with, the established policies and procedures. It is critical that the internal audit function is independent from the day-to-day functioning of the bank and that it has access to all activities conducted by the banking organisation, including at its branches and subsidiaries.
>
> The focus on the internal audit role in monitoring the banks' systems of internal control is seen as crucial. In all organizations, the growing trend towards self-auditing imposes a level of responsibility on internal audit for educating management on the need for good controls and risks that arise where this factor is not duly appreciated. Brochures, presentations, skills workshops and close consultation with managers may be considered internal audit roles in this search for getting management committed to a clear control orientation. These initiatives, however, must be taken in such a way as to reinforce and not dilute the extensive responsibilities of management for controlling resources. In the context of governance standards, controls have a focus on many aspects of an organization. The IIA's Performance Standard 2130.A1 provides four key aspects of the scope of controls by indicating that The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organization's governance, operations and IA regarding the:
>
> - reliability and integrity of financial and operational information;
> - effectiveness and efficiency of operations;
> - safeguarding of assets; and
> - compliance with laws, regulations and contracts.

The IIA goes on to make quite clear that the nature of internal audit's work means that even when internal audit is working on consulting engagements, there is still the need to consider whether controls are sound, so that efforts from consulting engagements can inform assurance work:

> ***2130.C1*** – During consulting engagements, internal auditors must address controls consistent with the engagement's objectives and be alert to significant control issues.
>
> ***2130.C2*** – Internal auditors must incorporate knowledge of controls gained from consulting engagements into evaluation of the organization's control processes.

Building the Control Model

One important feature of control relates to the need to contain activity within set limits or boundaries. We can amend our model to incorporate these limits in Figure 4.2.

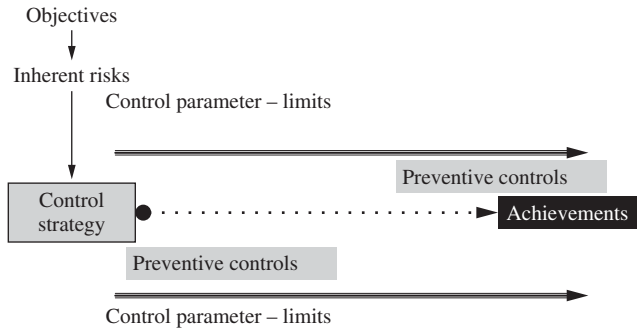


FIGURE 4.2 Internal control (2).

So activity moves an organisation towards achieving its objectives, by keeping within prescribed standards. The dotted black line moves dead straight to the achievement box and preventive controls are set which ensure everything is contained with the upper and lower control parameters. Constraining, containing and restricting controls are applied at the boundaries to ensure that only the right people get into the organisation, they only do the right things and they cannot access anything that falls outside their remit. Note that Section 4.6 provides more detail about different types of controls. The trend towards devolved organisations where each business unit is pretty well autonomous depends on a series of boundaries set at local levels throughout the organisation. Each local unit has its own perception of how these boundaries should be set, and how much leeway is given on either side of the limits. There is some move towards recentralising some of the support services and so making corporate alignment much easier. This trend has been noted by some writers, for example:

> Something odd seems to be going on. After spending the best part of two decades decentralising everything they could and allowing individual business units to operate almost as independent companies, a growing number of organisations are coming round to the view that fragmentation may not be a good idea after all. Some are taking personnel, finance and other specialist functions away from their business units and national subsidiaries and are setting up 'shared service' centres for the whole organisations. Others are bringing together different sections of the business by developing shared values and common employment practices, without necessarily changing structures. In many cases a single corporate brand provides the 'glue' that holds the organisation together.[8]

Making Controls Work

Control may be seen as one of the single most important topics that the auditor needs to master. The main justification for the internal auditing function revolves around the need to review systems of internal control with all other audit activities being, to an extent, subsidiary to this task.

A good understanding of the concept of control and how controls may be applied in practice is an important skill that takes many years to fully acquire. There are a number of issues that underlie the concept of controls:

- Controls are all means devised to promote the achievement of agreed objectives. This is an extremely broad interpretation of the control concept that, in theory, brings into play everything that management does in pursuing its objectives. We will return to this issue later.
- All controls have a corresponding cost and the idea is that the ensuing benefits should be worth the required outlay. Costs may be defined to include actual additional expenditure as in the case of a security officer employed to enhance controls over the safety of portable, moveable equipment held in offices. On the other hand costs may simply relate to the increased efforts applied by management in seeking compliance with, for example, a new document-signing procedure that makes it easier to find out who was involved in a certain transaction. The types of controls that spring to mind during a typical systems audit must be set within the cost context if the ensuing recommendations are to have any real use. Moreover, we must remember that these additional costs are borne by management and not the auditor.
- Controls belong to those who operate them and should not be viewed in isolation. In this respect, management is responsible for the controls, and the success of its operations will be linked to the degree to which controls work. There is a view that there are certain 'audit requirements' that have to be acted on when considering controls over operations. This term is, in reality, a fallacy since it implies that certain control criteria are not under management's responsibility but are in some way under the purview of internal audit. So, for example, audit may state that managers must install a mechanism that enables them to know the whereabouts of portable PCs at all times. To suggest that this is an audit requirement rather than a management procedure is to relieve management of this responsibility, and so distort the control orientation. The temptation to issue 'audit instructions' should be resisted as it will bring this inconsistency into play.
- Internal control is all about people, since controls work well only if they are geared to the user's needs in terms of practicality and usefulness. What appears sound on paper may be very difficult to put into practice. One may recall the newly appointed auditor who asks the cashier to record all cheques posted out each day, only to be told that it would take a certain type of individual to be able to log thousands of items daily. Again a detailed user manual that explains how a computerized system may be operated is of little use where the staff using the system have no real IT competence. Likewise, controls that involve an officer monitoring staff by observing their every movement may be very difficult to apply in practice. Where an auditor comes across staff who are not at all motivated then he/she may find a level of non-compliance that may be difficult to explain. The 'people factor' must be properly recognized. This comes to the fore when a change programme is being developed, and new systems and procedures are installed within a short time frame. The principle may be taken to the extreme where we might argue that if the right people are employed, then they will seek to develop their own controls as part of their everyday responsibilities. Unfortunately, the converse would be true where inadequate staff are taken on.
- Overcontrol is as bad as undercontrol in that it results in an impression that someone, somewhere is monitoring activity whereas this may not be the case in reality. Burdensome controls reduce the efficiency of operations and create an atmosphere of extreme bureaucracy where everything has to be signed for in triplicate. We have all read novels where the fictional police detective makes all the important arrests by refusing to 'do things by the book'. The other danger with overcontrol stems from a view that someone else will provide the necessary

checks and balances. This appears where accounts fail to reconcile but because so many parties become involved in the balancing process, differences are left in suspense on the basis that they will be corrected somewhere along the line. Where front line managers do not take responsibility for controlling their areas of work, but rely on a whole army of control teams, we again have a recipe for disaster. An example follows:

> An auditor in a large organization came across a finance officer who spent all his time checking in detail, mileage claims submitted by front line staff. He expressed concerns about the accuracy of a number of regular claims by certain officers and showed a few examples to the auditor. The auditor suggested that the manager who had approved the claims should be held accountable. It turned out that this manager did have some worries about the claims but felt that this would be picked up in finance and so signed them off. The extra control exercised by finance was actually stifling the main control, that is, managerial review.

- Entropy is the tendency to decay, and all control systems will underachieve where they are not reviewed and updated regularly. This is a quite straightforward concept that simply means that controls fall out of date as risks change and systems adapt to the latest environmental forces. Control routines fall into disuse over time, while new developments call for a change in control orientation. Most organisations have devolved their support functions to business unit level where what used to be corporate controls now fall under the remit of local business managers. The traditional control disciplines over, say, hiring and firing staff are no longer relevant in this new climate where local management has much devolved power. If the control orientation (say, better corporate standards) does not alter to reflect these types of developments then problems can ensue. Returning to the micro level, we can suggest that every time a form falls into disuse, this represents a symptom of entropy at work. There is an argument for getting management to consult with internal audit on all material proposals for restructuring and new systems installations, so that these issues may be considered. An alternative would be to educate management in the various control techniques as part of an ongoing development programme. Here we would expect all feasibility studies to contain a section covering 'risk assessed implications' that addresses any shift in balance of control as a mandatory consideration.
- The organisational culture affects the type of control features that are in place, which may be bureaucratic or flexible in nature. There is no one right answer since each activity will have its own control policies. This principle can be seen in a stark example whereby two different personnel sections were visited to cover an audit of recruitment practices with the following result:

> The first section consisted of seven staff squeezed into a small area with files and boxes scattered throughout the four offices. Personnel officers ran around making tea and discussing cases while making regular searches for misplaced files. The other section held six timesheeted personnel staff who sat in tidy offices that generated a feel of efficient working practices. Control in the first scenario centred around regular meetings and close contact between the personnel manager and staff. The other section, in contrast, operated controls based on formal reports of activities via timesheeted hours, with very little open communication. Different types of controls work for different environments and this fact must be acknowledged by the auditor if there is to be any value derived from the audit work.

One way of viewing the control system is to consider that each operation must be accompanied by a corresponding control system that is superimposed on the operation itself. In this way, control should not be an alien concept that impinges on the activity being performed, but a way of managing risks to the operation. System's objectives should be dependent on the underlying control objectives with each working in harmony to ensure that activities are undertaken in a controlled fashion. We can argue that assets can be acquired so long as they are used for authorized purposes, reports prepared so long as they are accurate and useful and operations managed so long as this is done in an efficient fashion. In this way, control follows risk to the activity. The only way to make managers responsible for control is to incorporate the key concerns within their objectives. So an objective to achieve something must also incorporate a requirement to do so, having due regard to matters of regularity, efficiency, compliance with procedure and overall control.

Building on the above point, the four main control objectives (see IIA standard 2130.A1) should always be kept in mind when considering and evaluating a system. In this way, management would have to ensure that in pursuing their goals, there is due regard to:

- reliability and integrity of financial and operational information;
- effectiveness and efficiency of operations;
- safeguarding of assets;
- compliance with laws, regulations and contracts.

The growing recognition of chaos management brings with it a need to control what appears at first sight a situation out of control. This may be the single biggest challenge now facing internal audit. A bottom-line control given to a business unit may simply be encompassed in a defined gross profit margin and nothing else. Controls that do not impact on this figure may be deemed to have no relevance at all. This may result in a chaotic search for profits that has no regard for the traditional controls of authorization, good documentation, supervision, reconciliation and so on. It may even be accepted that a line manager may abuse company resources so long as this profit target is met. The concept of control will be much different in this type of environment and this must be recognized. Many of the moves towards good corporate governance are based on the growing recognition that there must be some standards of conduct outside the bottom-line profit margin. The question of whether there is a right way of doing things is fundamental to any discussion of controls. One answer is to suggest that since controls are means by which objectives are achieved, they must link directly into these goals to be of any use. If these goals are single-issue based, then so will be the types of controls that support them.

4.2 Control Framework – COSO

The wide view of controls means that internal controls cover all aspects of an organisation and there is a clear need for a way of pulling together control concepts to form an integrated whole, that is a control framework. COSO of the Treadway Commission devised one such model that has an international recognition as a useful standard. All larger organisations need a formal control framework as a basis for their systems of internal control. IIA Performance Standard 2120.A4 notes the importance of a set of organisational criteria that the auditor can use to review control systems (www.coso.org):

> Adequate criteria are needed to evaluate controls. Internal auditors should ascertain the extent to which management has established adequate criteria to determine whether objectives and goals have been accomplished. If adequate, internal auditors should use such criteria in their

> evaluation. If inadequate, internal auditors should work with management to develop appropriate evaluation criteria.

This is not always easy; Jeff Gibbs and Susan Gibson have warned about the risk of viewing controls as a series of isolated devices dotted around the organisation:

> If internal auditing is to perform effective audits of the internal control system, management and the board must adopt, implement and operate within a framework of control. Otherwise, internal auditing is faced with the difficult task of evaluating a system for which there is no foundation. Without a framework that management is committed to and feels accountable for, any audit effort is unlikely to succeed. Both the COSO report . . . and the CoCo document . . . have established and defined overall frameworks and philosophies that organizations use to manage risks and achieve objectives . . . Organizations that have postponed adopting a control model because of inabilities to audit soft controls may want to re-think their position. Direct audit approaches for assessing the effectiveness of soft controls now exist and can supplement the CSA approach employed by many organizations. Internal auditors play an important role in monitoring and evaluating the control system, including soft controls. Those who add these tools to their arsenal are poised to make an even greater contribution to the success of their organizations.[9]

This point is crucial to understanding the new-look internal auditing. In the past the silo approach has been to consider whatever individual system we were auditing at the time. Systems were defined and audited, while the resultant report detailed the weak areas and how they could be improved. There is no possible way the aggregation of separate internal audit reports over a period could be used to comment on the overall state of controls in an organisation. It is only by considering the adopted control model that the internal auditor is able to make board level declarations concerning internal control. The need to focus on a control framework has been described in the IIA Handbook on *Implementing the Professional Practices Framework* where it has been made clear that:

> Highly touted management control frameworks like COSO, Cadbury, and CoCo have exposed the futility of considering control activities in a vacuum. To be their most effective, controls should be aligned with the broad objectives of the organisation and the risks of not achieving those objectives. The role of control in the organisation is, therefore, not limited to ensuring financial integrity and compliance with polices and procedures within functional silos, and neither is the role of the internal auditor. Instead, internal control and the internal audit activity exist to help the organisation manage all of its risks and promote effective governance . . . Due to this non-risk focused perception of internal control, many internal auditors fell into the practice of simply assuming that the procedures and rules – the controls – put in place by an organisation were the right ones for the business. As a result, their control assessments were designed primarily to make sure that individuals within a particular function performed their jobs in the manner they were instructed . . . The rise and fall of any organisation is directly related to the effectiveness of its risk, control and governance systems. Because it is now required to more proactively serve the very structure holding the organisation together, internal auditing has never been more valuable.[10]

In fact, we can develop our control model to reflect the valuable platform provided by the control framework in Figure 4.3.

The control framework needs to be in place to promote the right control environment. Some might argue that the control environment in turn inspires an organisation to build a suitable framework, although we will see that our first framework, COSO, incorporates the control

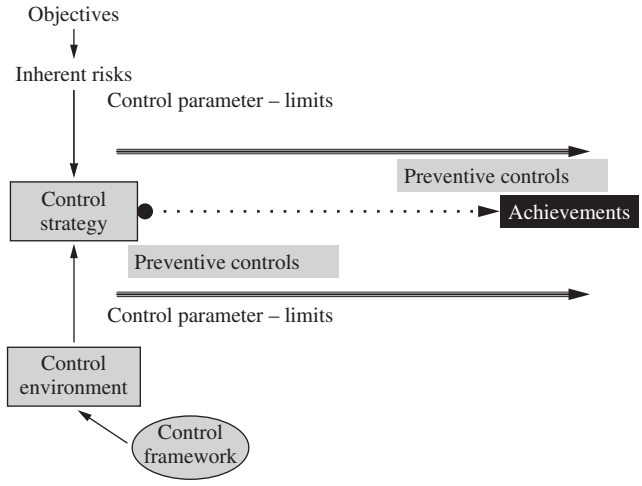


FIGURE 4.3 Internal control (3).

environment as a separate component. The framework drives the environment, which in turn enables an organisation to develop its control strategy in response to the assessment of various risks to achieving objectives. Risk assessment and control design is fragmented when not attached to a clear control framework and any audit effort not directed at the big picture will itself be less valuable. The next areas to cover are based around the COSO components and the entire model is shown in Figure 4.4 before we describe each part.

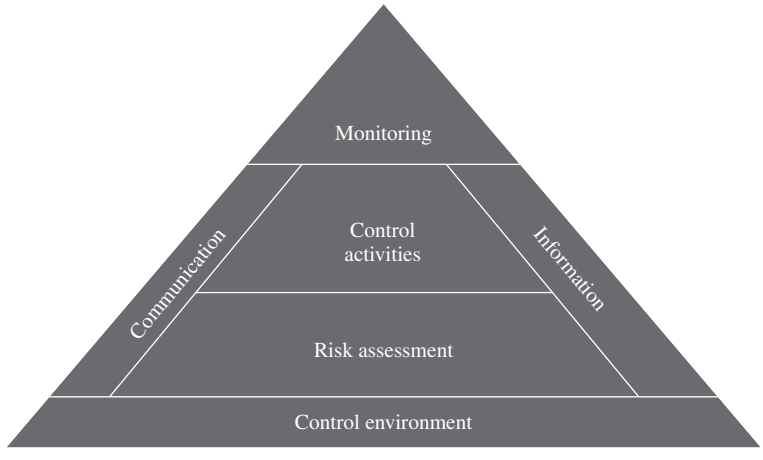


FIGURE 4.4 The COSO model.

The COSO website (www.coso.org) gives the official background to their work:

> In 1985, the National Commission of Fraudulent Financial Reporting, known as the Treadway Commission, was created through the joint sponsorship of the AICPA, American Accounting Association, Financial Executives International (FEI), IIA and Institute of Management Accountants.

> On the basis of its recommendations, a task force under the auspices of the COSO conducted a review of internal control literature. The eventual outcome was the document *Internal Control – Integrated Framework*. COSO emphasised the responsibility of management for internal control.
>
> Definition – Internal control is a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
>
> - effectiveness and efficiency of operations
> - reliability of financial reporting
> - compliance with applicable laws and regulations.
>
> Internal control is a process because it is not an event of circumstance but a dynamic concept – nor is it simply a set structure.

The idea is to arrive at a commonly understood definition of internal control since, in the words of COSO: 'internal control means different things to different people'. There are many internal auditors who support the use of a defined control model, including Mark R. Simmons who has written:

> By taking the manager's perspective the (COSO) Framework elevates the level at which auditors look at internal control from a traditional, operational level to a more strategic level. The beauty of the Framework is that although there is a shift in emphasis, it can be applied to audits of entire organizations, or to audits of individual organizational units, in a strategic way. By using controlled and directed focus groups as a primary means to gathering evidence about the state of control, the Framework gives even small audit shops the capability to conduct timely, comprehensive audits. The Framework provides internal auditors with an excellent methodology for adding significant value to the organization, while maintaining compliance with the Standards for the Professional Practice of Internal Auditing.[11]

Each component of the COSO model is dealt with next.

Control Environment

Turning once again to the COSO website, their summary of the control environment follows:

> The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values and competence of the entity's people; management's philosophy and operating style; the way management assigns authority and responsibility, and organizes and develops its people; and the attention and direction provided by the board of directors.

Meanwhile, we can restate the IIA definition of this control environment as:

> The attitude and actions of the board and management regarding the significance of control within the organization. The control environment provides the discipline and structure for the achievement of the primary objectives of the system of internal control. The control environment includes the following elements:
>
> - Integrity and ethical values.
> - Management's philosophy and operating style.

- Organizational structure.
- Assignment of authority and responsibility.
- Human resource policies and practices.
- Competence of personnel.

The control environment is the main platform upon which the rest of the control framework is built. In fact, there is a strong argument that if we can get the control environment right then everyone at whatever level they sit in the organisation will construct the rest of the COSO framework themselves. To build a comprehensive picture of a positive control environment we can list the many types of organisational attributes (in no particular order) that together form this much-sought-after condition:

- A supportive view of internal control throughout the organization.
- Board level involvement in setting standards for sound systems of internal control, with responsibility residing with the chief executive.
- Capable staff who have formal competencies defined, including those relating to a good understanding of risk assessment, risk management and internal controls. Managers should have clear accountability for internal control in their areas of work.
- Clear and consistent corporate objectives that can be driven down and across the organisation with an overall mission and vision that reaches all parts of the organisation.
- Clear understanding of role and responsibilities and accountabilities among managers and employees.
- Continuous learning ethos based on good staff development and positive performance management systems that have a longer as well as shorter term focus; and continuous corporate improvements including improved IS and development projects.
- Decision-making processes that take account of risk, financial implications, authority levels and the need for transparency. Any decision involving control override should be specially scrutinized and formally authorized at the appropriate level. In general, control override should be discouraged as should any effort to 'get around the system'.
- Easy-to-use and respected reporting arrangements for fraud, irregular activities or problems that are not being resolved.
- Effective communications that impact all directions in the organisation and that encourage openness and transparency even where this involves giving bad news to senior management.
- Executive management team that has continuity and good working relations and credibility among employees.
- Formal and fair human resource policies (recruitment, induction and development) that promote a developed and dedicated staff who have good role definition and are empowered but supported. The HR policies should ensure undesirable people are 'found out' at recruitment stage by extensive checks or disciplined if they start work for the organisation. Also a process to find out whether staff dissatisfaction and high turnover are linked to poor controls.
- Formal planning systems with workable targets that take on board risk assessments and the available resources. These systems should provide effective feedback to all involved.
- Good awareness of financial systems and how they feed into the final accounts that revolve around formal financial regulations.
- Good understanding of the role of internal and external audit and direct access to advice, information and consulting services and positive responses to audit recommendations.
- Good use of staff attitude surveys that serve to promote good morale among staff and action taken to improve known problems.

- Knowledge management and continuity arrangements for ensuring experience of key people is harnessed, shared and maintained by the organisation.
- Positive view on the need for effective management of risk.
- Responsible approach to office arrangement with tidy desks and people taking responsibility for security, storing valuable items, covering each other and helping out.
- Responsive mechanisms to incorporate regulatory and other compliance issues into organisational practices. Also arrangements for promoting compliance with set standards and controls that allow problems to be communicated upwards and acted on where significant.
- Responsive organisation structure that is developed around defined roles and has a good balance of centralized and decentralized control standards and suitable supervisory reviews where appropriate. Head office will need strong communication links with local offices and any delegations should be monitored for results and areas for improvement.
- Robust and rigorous external audit process that addresses any factors that facilitate the possibility of financial misstatement.
- Robust complaints procedure that is used to help manage risks to the service in question.
- Sensible use of delegation with clear authorization for spend and budgets that are monitored and managed in line with clear standards with action taken on potential overspends.
- Separation of duties for operations that are key to success or involve material resources and information.
- Sound and reliable IS that feeds into decision-making and controls.
- Tone set by the top reflects strong ethical standards that are realistic and driven down through the organisation.
- Well-developed monitoring and review arrangements for key processes with problems aggregated and accelerated upwards where appropriate.
- Well-developed performance management system that reflects defined responsibilities and fair rewards and is linked in the risk management process.
- Well-developed value system that forms the basis of a formal code of conduct that is taken seriously from the top and is action oriented where there are problems.
- Well-established audit committee that meets best practice standards in discharging its oversight role.

Risk Assessment

The COSO website provides a summary of where risk assessment fits into the control equation:

> Every entity faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is establishment of objectives, linked at different levels and internally consistent. Risk assessment is the identification and analysis of relevant risks to achievement of the objectives, forming a basis for determining how the risks should be managed. Because economic, industry, regulatory and operating conditions will continue to change, mechanisms are needed to identify and deal with the special risks associated with change.

The risk assessment stage arises naturally from the control environment where people want to get their control right by focusing on prioritized risks. This has been covered in the previous chapter and essentially requires that:

- risks are identified and analysed in respect of their impact on business objectives;
- risks are assessed so that they can be prioritized for impact and likelihood;

- steps are taken to work out how best to manage the risks having regard to respective responsibilities and the definition of risk owners;
- required action is incorporated into planning and performance systems used by the organisation;
- risk registers are prepared that support the assurance reporting systems for corporate governance codes;
- continuous effort is made to update the risk assessment in line with changes that impact on the organisation and expectation of stakeholders;
- efforts are made to ensure buy-in and counter any inertia for the risk management process across the organisation.

Control Activities

The COSO website provides a summary of where this aspect fits into their model:

> Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.

The COSO model requires controls to be designed to counter unacceptable levels of risk that have been identified during the risk assessment stage. Note that a later section will cover detailed control mechanisms or activities as they are termed here.

Information and Communication

The COSO website provides a summary of where this aspect fits into their model:

> Pertinent information must be identified, captured and communicated in a form and timeframe that enable people to carry out their responsibilities. Information systems produce reports, containing operational, financial and compliance-related information, that make it possible to run and control the business. They deal not only with internally generated data, but also information about external events, activities and conditions necessary to informed business decision-making and external reporting. Effective communication also must occur in a broader sense, flowing down, across and up the organization. All personnel must receive a clear message from top management that control responsibilities must be taken seriously. They must understand their own role in the internal control system, as well as how individual activities relate to the work of others. They must have a means of communicating significant information upstream. There also needs to be effective communication with external parties, such as customers, suppliers, regulators and shareholders.

Information should be recorded and communicated to management and others within the organisation who need it and in a form and within time frames that enables them to carry out their internal control and other responsibilities. Exchange of useful information between and among people and organisations to support decisions and coordinate activities include:

- flexible use of options including verbal or in writing, formal and informal;
- information on risks and changes in internal and external factors that impact on risk profiles;

- time frame appropriate for the use designed for;
- efficient mechanisms to identify, capture and communicate information between different parts of the organisation;
- dissemination of the control policy to all staff, and training support in delivering key messages in the control policy where appropriate;
- operational, strategic and financial information;
- reports on the extent to which controls are adhered to and special purpose reports on breaches and control override – including exception reports that show deviation from plan and point to any required interventions;
- informal gossip and conversations between employees at all levels in the organisation;
- set criteria for IS covering the need to be accurate, valid, authorized, complete, processed properly, to support decision-making and compliance systems;
- clear feeds from operating systems into financial systems and the final accounts;
- special purpose reports designed by the user;
- corporate standards on information covering legal requirements, access, security, usage, retention, disclosure, validity checks, confidentiality, and so on;
- upwards communications systems that can be used in conjunction with control self-assessment events that encourage middle management to respond and address issues raised;
- downwards communication that sends clear messages and information to build energies around the corporate strategy and set out senior managements' top risk priorities for consideration and action;
- feedback mechanisms built into communication networks to ensure that message is understood and to allow for adjustment if required, effective feedback being an important component of internal control;
- communications systems that allow good contact with stakeholders outside the organisation;
- good communication with the internal and external auditors who have a clear platform to comment and engage on risk- and control-related issues;
- communications based on value systems that derive from the control environment;
- robust IS that support the communication needs and provide fast and reliable infrastructures that flex to fit changing circumstances;
- development of web-based communications with close contact with partners, associates and customers, allowing interactive communications that allow customers to build their product and secure a unique service from the organisation.

Monitoring

The COSO website provides a summary of where this aspect fits into their model:

> Internal control systems need to be monitored – a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two. Ongoing monitoring occurs in the course of operations. It includes regular management and supervisory activities, and other actions personnel take in performing their duties. The scope and frequency of separate evaluations will depend primarily on an assessment of risks and the effectiveness of ongoing monitoring procedures. Internal control deficiencies should be reported upstream, with serious matters reported to top management and the board. There is synergy and linkage among these components, forming an integrated system that reacts dynamically to changing conditions. The internal control system is intertwined with the entity's operating activities and exists for fundamental business reasons.

> Internal control is most effective when controls are built into the entity's infrastructure and are a part of the essence of the enterprise. 'Built in' controls support quality and empowerment initiatives, avoid unnecessary costs and enable quick response to changing conditions. There is a direct relationship between the three categories of objectives, which are what an entity strives to achieve, and components, which represent what is needed to achieve the objectives. All components are relevant to each objective's category. When looking at any one category – the effectiveness and efficiency of operations, for instance – all five components must be present and functioning effectively to conclude that internal control over operations is effective.

Internal control monitoring should assess the quality of performance over time and ensure that the findings of audits and other reviews are promptly resolved:

- Everyone should have a clear responsibility for monitoring their work and work of others as a natural consequence of the way work is organised.
- Staff should assess risks to achieving their objectives and monitor the way controls act to mitigate these risks.
- There should be clearly defined roles for staff with supervisory responsibilities with examples of the types of checks that should be made, ongoing support that should be given to front line staff and care taken to ensure compliance with procedure.
- The use of inspections and random checks should be applied to high risk areas and there should be regular contact between head office and local units. Management by walking around is highly recommended.
- Management should seek to secure independent evidence that controls are working as prescribed in a fair and positive manner. Staff should be told that these checks will be made and to cooperate fully. Problem areas should be given greater attention.
- Formal lines of communication should be established to address concerns that need to be accelerated upwards, including a whistle-blowing line for unresolved problems and control weaknesses.
- Random checks should be made on use of IS to isolate unauthorized activity as well as for routine monitoring of computer interactions to check consistency with organisational policies.
- There should be regular communication with the board to help them discharge their role to oversee the system of internal control.
- Formal monitoring role should be located at board level, which may be resourced through a defined compliance officer, charged with ensuring standards are adhered to and people know what is required to meet regulatory and legal obligations. Compliance may have an educational role but must also have enough teeth to act in case of serious breaches and negligence.
- Formal reporting lines should be created for support activities such as human resources to ensure poor practices in business units can be isolated and remedied.
- Constant scanning should take place to determine whether aspects of supervision and review can be discarded or reduced without any adverse effects.
- Professional and dynamic internal audit process that seeks to support self-assessment and review among managers and their teams should be in place.
- Formal review mechanisms should be built into project management to ensure progress is considered and quality issues resolved.
- Careful consideration of complaints from customers and others should take place to assess implications for the functioning of internal controls.
- There should be robust use of exception reporting where variances in budgeting systems, performance measures, quality targets and planning systems to highlight problems and ensure action-oriented solutions are devised.

- A formal system of assurance reporting should be introduced, where internal control statements are signed by senior management on the basis of their monitoring activities over internal controls.
- All new systems should be designed with suitable controls and mechanisms to allow monitoring and authorizations for material transactions.
- An efficient process for addressing gaps in controls and failures that have been identified by stakeholders (e.g. customers, suppliers, etc.), employees or auditors and consultants should be introduced.
- There should be careful consideration of different sources of information so that discrepancies can be followed up and addressed.
- Good use of reconciliations of records for physical resources such as stores, cash, equipment and speedy follow-up of discrepancies should take place.
- Dynamic audit committee should be formed with a role in ensuring that monitoring systems work well and high risk problems are made known to senior management. The audit committee will also want to see that the control framework is working well.
- Awareness training should be made available for managers and supervisors on the techniques available to monitor and inspect routines and the need to install competencies in all staff relating to this aspect of control.
- Performance evaluation systems should involve monitoring of KPIs and whether they are likely to be achieved.
- Monitoring arrangements should be integrated with initiatives to empower people to take decisions and drive the business forward. All new initiatives should have an associated process for monitoring use or resources, success criteria and whether policies and procedures are being followed.

The COSO model is quite dynamic in that it covers most aspects of structures and processes that need to be in place to provide control. It is difficult to know how a board can state that it has reviewed its systems of internal control without reference to a comprehensive model or criteria for evaluating these controls at a corporate level. COSO simply asks five key questions:

1. Do we have the right foundations to control our business? (control environment)
2. Do we understand all those risks that stop us from being in control of the business? (risk assessment)
3. Have we implemented suitable control activities to address the risks to our business? (control activities)
4. Are we able to monitor the way the business is being controlled? (monitoring)
5. Is the control message driven down through the organisation and associated problems and ideas communicated upwards and across the business? (communication and information)

If we can assess the quality of the responses to these five questions, we are on the way to achieving control and being able to demonstrate to all parties that their business concerns are in safe hands, even though no absolute guarantees are possible.

4.3 Control Framework – CoCo

The COSO framework is a powerful tool in that it allows an organisation to focus on key structures, values and processes that together form this concept of internal control, far outside the narrow financial focus that used to be the case. The individual is part of the process but it can be

hard to get a corporate solution down to grass roots. The criteria of control (CoCo) is a further control framework that can mean more to teams and individuals and includes an interesting learning dynamic. CoCo was developed by the Canadian Institute of Chartered Accountants (CICA) and is now an international standard. The CICA website (www.cica.ca) gives an account of their understanding of control as a platform for the criteria that was developed:

> Control needs to be understood in a broad context. Control comprises those elements of an organization (including its resources, systems, processes, culture, structure and tasks) that, taken together, support people in the achievement of the organization's objectives. The effectiveness of control cannot be judged solely on the degree to which each criterion, taken separately, is met. The criteria are interrelated, as are the control elements in an organization. Control elements cannot be designed or evaluated in isolation from each other. Control is as much a function of people's ethical values and beliefs as it is of standards and compliance mechanisms. Control should cover the identification and mitigation of risks. These risks include not only known risks related to the achievement of a specific objective but also two more fundamental risks to the viability and success of the organization:
>
> 1. failure to maintain the organization's capacity to identify and exploit opportunities;
> 2. failure to maintain the organization's capacity to respond and adapt to unexpected risks and opportunities, and make decisions on the basis of the telltale indications in the absence of definitive information.
>
> The board of directors should assess the effectiveness of control – CoCo principles of assessment:
>
> - The assessment focuses on significant objectives of the organization and the management of risks related to such objectives.
> - The assessment is from the perspective of the organization as a whole.
> - The assessment is the responsibility of the chief executive officer.
> - The assessment uses a thorough and trustworthy process that incorporates the perspective of people from throughout the organization.
> - The assessment is based on the CICA criteria of control framework.
> - The assessment is conducted by people with the appropriate skills, knowledge, qualities and perspectives.
> - The assessment includes reporting the results of the assessment to the board of directors.
> - The assessment process is reviewed to learn how the assessment might have been improved.

The principles may be organised according to the four groupings of the CICA criteria of control framework as illustrated in Figure 4.5.

The main components are explained below:

Purpose The model starts with the need for a clear direction and sense of purpose. This includes objectives, mission, vision and strategy; risks and opportunities; policies; planning; and performance targets and indicators. It is essential to have a clear driver for the control criteria and since controls are about achieving objectives, it is right that people work to the corporate purpose. Much work can be done here in setting objectives and getting people to have a stake in the future direction of the organisation. The crucial link between controls and performance targets is established here as controls must fit in with the way an organisation measures and manages performance to make any sense at all.

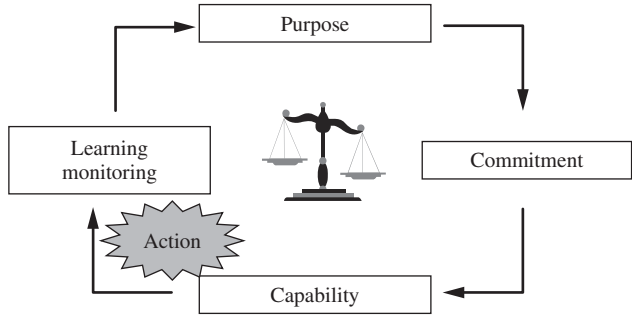


FIGURE 4.5 The CoCo model.

Commitment The people within the organisation must understand and align themselves with the organisation's identity and values. This includes ethical values, integrity, human resource policies, authority, responsibility and accountability, and mutual trust. Many control systems fail to recognize the need to get people committed to the control ethos as a natural part of the way an organisation works. Where people spend their time trying to 'beat the system', there is normally a lack of commitment to the control criteria. The hardest part in getting good control is getting people to feel part of the arrangements.

Capability People must be equipped with the resources and competence to understand and discharge the requirements of the control model. This includes knowledge; skills and tools; communication processes; information; coordination; and control activities. Where there is a clear objective, and everyone is ready to participate in designing and installing good controls, there is still a need to develop some expertise in this aspect of organisational life. Capability is about resourcing the control effort by ensuring staff have the right skills, experience and attitudes not only to perform well but also to be able to assess risks and ensure controls make it easier to deal with these risks. Capability can be assisted by training and awareness seminars, either at induction or as part of continuing improvement programmes.

Action This stage entails performing the activity that is being controlled. Before employees act, they will have a clear purpose, a commitment to meet their targets and the ability to deal with problems and opportunities. Any action that comes after these prerequisites has more chance of leading to a successful outcome.

Monitoring and learning People must buy into and be part of the organisation's evolution. This includes monitoring internal and external environments, monitoring performance, challenging assumptions, reassessing information needs and IS, follow-up procedures and assessing the effectiveness of control. Monitoring is a hard control in that it fits in with inspection, checking, supervising and examining. Challenging assumptions is an important soft control in that it means people can develop and excel. Each activity is seen as part of a learning process that lifts an organisation to a higher dimension. Some organisations employ people who have tried and failed to start their own high risk venture, on the basis that they have had invaluable experiences that, if they have learnt lessons from, will make them stronger and much more resilient in growing a new business. Organisations that are based around blame cultures will not encourage positive learning experiences, and will interpret controls as mechanisms for punishing people whose performance slips. The CoCo criteria encourages a positive response to feedback on activities.

This emphasis on 'soft controls' as well as more traditional ones is an important aspect of CoCo and these two philosophies of control have been explained by Peter Jackson, Director of Criteria of Control at CICA, and are summarized as follows:

> Scientific – hard controls:
>
> - People are inherently dishonest, lazy and eager, if possible, to avoid fulfilling commitments that involve effort.
> - The organization is a machine.
> - Control is effective when employees do as they are told by management.
>
> Humanistic – soft controls:
>
> - People are honest, hardworking, and fulfil their commitments to the best of their ability.
> - The organization is a social organism.
>
> Control is effective when employees and management cooperate to achieve shared objectives.[12]

4.4 Other Control Models

COSO and CoCo are well-known control frameworks and they provide most of what is needed for an organisation to consider when developing its own framework. There are, however, other sources of information to assist this task of getting control understood, addressed and reported.

The International Organisation of Supreme Audit Institutions

This body has prepared a standard on internal control that provides a foundation for accountability in government that covers the following ground:

> Managers are responsible for establishing an effective control environment in their organizations. This is part of their stewardship responsibility over the use of government resources. Indeed, the tone managers set through their actions, policies, and communications can result in a culture of either positive or lax controls. Planning, implementing, supervising, and monitoring are fundamental components of internal control. You may go about these activities routinely, without thinking of them as part of a broad control environment that helps to ensure accountability. Checklist for Manager:
>
> 1. In establishing your framework, have you:
>   - Assessed the risks the organization faces?
>   - Identified control objectives to manage the risks?
>   - Established control policies and procedures to achieve the control objectives?
>   - Created a positive control environment?
>   - Maintained and demonstrated personal and professional integrity and ethical values?
>   - Maintained and demonstrated an understanding of internal controls sufficient to effectively discharge responsibilities?
> 2. For implementing internal control, have you:
>   - Adopted effective internal control throughout the organization?
>   - Based the organization's internal control on sound control standards?

- Included in the organization's internal control structure appropriate and cost-effective control practices?
- Prescribed control practices through management directives, plans, and policies?
- Established a means of continually monitoring the operation of the organization's internal control practices?

3. Concerning the audit function, have you:
   - Shown an understanding of the difference between internal control and internal audit?
   - Recognized that an audit function is integral to your organization's internal control?
   - Established an audit function?
   - Ensured the audit organization's independence?
   - Given the audit organization responsibility for evaluating the effectiveness of the audited organization's internal control practices?
   - Established a system to monitor the organization's progress in implementing internal and external auditor recommendations.[13]

Control Objectives for Information and Related Technology (COBIT)

This control standard, known as COBIT, covers security and control for IT systems in support of business processes and is designed for management, users and auditors. Several definitions are applied to this standard including:

- **Control:** The policies, procedures, practices and organisational structures designed to provide reasonable assurance that business objectives will be achieved and that undesirable events will be prevented or detected and corrected.
- **IT control objective:** Statement of the desired results of purpose to be achieved by implementing control procedures in a particular IT activity.
- **IT governance:** A structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus returns over IT and its processes.

The standard argues that there are certain critical success factors to reflect the critical importance of IT systems. The success factors cover the following areas:

- IT governance activities are integrated into the enterprise governance process and leadership behaviours.
- IT governance focuses on the enterprise goals, strategic initiatives, the use of technology to enhance the business and on the availability of sufficient resources and capabilities to keep up with business demands.
- IT governance activities are defined with a clear purpose, documented and implemented, based on enterprise needs and with unambiguous accountabilities.
- Management practices are implemented to increase efficient and optimal use of resources and increase the effectiveness of IT processes.
- Organisational practices are established to enable sound oversight; a control environment/culture; risk assessment as standard practice; degree of adherence to established standards; monitoring and follow-up of control deficiencies and risks.
- Control practices are defined to avoid breakdowns in internal control and oversight.
- There is integration and smooth interoperability of the more complex IT processes such as problem, change and configuration management.

- An audit committee is established to appoint and oversee an independent auditor, focusing on IT when driving audit plans, and review the results of audits and third-party review.

COBIT has four main components (domains) and for these domains there are a further 34 high level control processes:

- planning and organisation
- acquisition and implementation
- delivery and support
- monitoring.

Basel Committee on Banking Supervision

This section reflects the work on internal controls for banking organisations developed by the Basel committee on Banking Supervision, which is a committee of banking supervisory authorities established by the central bank governors of a group of leading countries in 1975. It consists of senior representatives of bank supervisory authorities and central banks from Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, the Netherlands, Sweden, Switzerland, the United Kingdom and the United States. It usually meets at the Bank for International Settlements in Basel, where its permanent secretariat is located. The Basel committee view a system of effective internal controls as a critical component of bank management and a foundation for the safe and sound operation of banking organisations. While the committee has adopted COSO in that it assesses internal control under the five main headings of the COSO model, it is, nonetheless, an important source of advice on control, particularly for the banking and financial services sectors. The committee describes the five COSO areas as:

1. management oversight and the control culture
2. risk recognition and assessment
3. control activities and segregation of duties
4. information and communication
5. monitoring activities and correcting deficiencies.

They argue that internal control is a *process* effected by the board of directors, senior management and all levels of personnel. It is not solely a procedure or policy that is performed at a certain point in time, but rather it is continually operating at all levels within the bank. The board of directors and senior management are responsible for establishing the appropriate culture to facilitate an effective internal control process and for monitoring its effectiveness on an ongoing basis; however, each individual within an organisation must participate in the process. They also note several common causes of control breakdowns in banks that suggest a failing of internal controls including:

- lack of adequate management oversight and accountability, and failure to develop a strong control culture within the bank;
- inadequate recognition and assessment of the risk of certain banking activities;
- whether on- or off-balance sheet transactions;
- the absence or failure of key control structures and activities, such as segregation of duties, approvals, verifications, reconciliations, and reviews of operating performance;

- inadequate communication of information between levels of management within the bank, especially in the upward communication of problems;
- inadequate or ineffective audit programs and monitoring activities.

The committee has spent some time developing principles of internal control that relate to the banking environment and selected extracts from these principles follow:

- **Principle 1:** The board of directors should have responsibility for approving and periodically reviewing the overall business strategies and significant policies of the bank; understanding the major risks run by the bank, setting acceptable levels for these risks and ensuring that senior management takes the steps necessary to identify, measure, monitor and control these risks; approving the organisational structure; and ensuring that senior management is monitoring the effectiveness of the internal control system. The board of directors is ultimately responsible for ensuring that an adequate and effective system of internal controls is established and maintained.
- **Principle 2:** Senior management should have responsibility for implementing strategies and policies approved by the board; developing processes that identify, measure, monitor and control risks incurred by the bank; maintaining an organisational structure that clearly assigns responsibility, authority and reporting relationships; ensuring that delegated responsibilities are effectively carried out; setting appropriate internal control policies; and monitoring the adequacy and effectiveness of the internal control system.
- **Principle 3:** The board of directors and senior management are responsible for promoting high ethical and integrity standards, and for establishing a culture within the organisation that emphasises and demonstrates to all levels of personnel the importance of internal controls. All personnel at a banking organisation need to understand their role in the internal controls process and be fully engaged in the process.
- **Principle 4:** An effective internal control system requires that the material risks that could adversely affect the achievement of the bank's goals are being recognised and continually assessed. This assessment should cover all risks facing the bank and the consolidated banking organisation (that is, credit risk, country and transfer risk, market risk, interest rate risk, liquidity risk, operational risk, legal risk and reputational risk). Internal controls may need to be revised to appropriately address any new or previously uncontrolled risks.
- **Principle 5:** Control activities should be an integral part of the daily activities of a bank. An effective internal control system requires that an appropriate control structure is set up, with control activities defined at every business level. These should include: top level reviews; appropriate activity controls for different departments or divisions; physical controls; checking for compliance with exposure limits and follow-up on non-compliance; a system of approvals and authorisations; and, a system of verification and reconciliation.
- **Principle 6:** An effective internal control system requires that there is appropriate segregation of duties and that personnel are not assigned conflicting responsibilities. Areas of potential conflicts of interest should be identified, minimised and subject to careful, independent monitoring.
- **Principle 7:** An effective internal control system requires that there are adequate and comprehensive internal financial, operational and compliance data, as well as external market information about events and conditions that are relevant to decision making. Information should be reliable, timely, accessible and provided in a consistent format.
- **Principle 8:** An effective internal control system requires that there are reliable IS in place that cover all significant activities of the bank. These systems, including those that hold and use data in an electronic form, must be secure, monitored independently and supported by adequate contingency arrangements.

- **Principle 9:** An effective internal control system requires effective channels of communication to ensure that all staff fully understand and adhere to policies and procedures affecting their duties and responsibilities and that other relevant information is reaching the appropriate personnel.
- **Principle 10:** The overall effectiveness of the bank's internal controls should be monitored on an ongoing basis. Monitoring of key risks should be part of the daily activities of the bank, as well as periodic evaluations by the business lines and internal audit.
- **Principle 11:** There should be an effective and comprehensive internal audit of the internal control system carried out by operationally independent, appropriately trained and competent staff. The internal audit function, as part of the monitoring of the system of internal controls, should report directly to the board of directors or its audit committee, and to senior management.
- **Principle 12:** Internal control deficiencies, whether identified by business line, internal audit or other control personnel, should be reported in a timely manner to the appropriate management level and addressed promptly. Material internal control deficiencies should be reported to senior management and the board of directors.
- **Principle 13:** Supervisors should require that all banks, regardless of size, have an effective system of internal controls that is consistent with the nature, complexity and risk inherent in their on- and off-balance-sheet activities and that responds to changes in the bank's environment and conditions. In those instances where supervisors determine that a bank's internal control system is not adequate or effective for that bank's specific risk profile (for example, does not cover all of the principles contained in this document), they should take appropriate action.

The all-important task of assessing internal control is supported by the Banks' Supervisory Authorities who should require that all banks, regardless of size, have an effective system of internal controls that is consistent with the nature, complexity and risk inherent in their on- and off-balance-sheet activities and that responds to changes in the bank's environment and conditions. In those instances where supervisors determine that a bank's internal control system is not adequate or effective for that bank's specific risk profile (for example, does not cover all of the principles contained in this document), they should take appropriate action.[14] Each organisation must decide what to do about its system of internal control. There are several options:

1. Do nothing. On the basis that individual controls are in place and working and that this is good enough to satisfy stakeholders.
2. Document the existing control arrangements and develop them further to reflect an agreed corporate internal control framework.
3. Invent a model. Each organisation may develop a unique perception of its controls and have this as its corporate internal control framework.
4. Adopt an existing published framework. Here the organisation will simply state that it has adopted COSO, CoCo or some version that the regulators promote.
5. Adapt an existing framework to suit the context and nuances of the organisation in question. An international control framework may then be used as a benchmark to develop a tailored framework that fits the organisation in question.
6. Selectively use all the available published material as criteria to develop a control framework that suits. Similar to 5 above but draws from all available sources of published guidance.

Whatever the chosen solution, each organisation should publish a policy on internal control and in developing the policy, it will become clear that decisions have to be made along the lines suggested by options 1 to 6.

4.5 Links to Risk Management

We may expand our control model to include two more features. The first is CRSA where inherent risks are considered and assessed in a workshop setting to ensure any controls that need updating are firmly related to the risks that have been debated. The second addition is the corporate governance arrangements involving the role and responsibilities of the main board and audit committee. Control models that fail to link their mission to the governance structures will flounder. In fact, it is the governance arrangements that drive the risk assessments, which in turn drives the adopted processes and controls put in place. In this way, the model assumes some depth and links the control effort back to the main board in Figure 4.6.

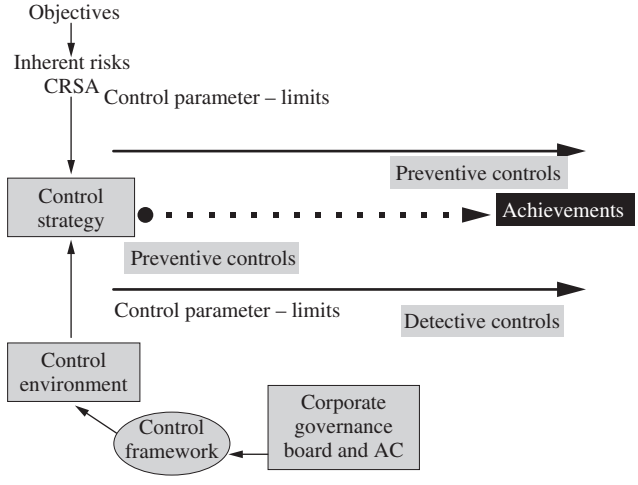


FIGURE 4.6 Internal control (4).

As suggested by the Basel committee, there are many things that can go wrong where suitable controls are not firmly in place. Where accountabilities are wrongly located, and excessive power is not held in check by balancing and checking forces, and where security is ignored and there is pressure to take convenient short cuts to accounting for income and expenditure, then there is likely to be problems. Moreover where controls do not work, or they can be overridden at a whim, then what looks good on paper may be useless in practice. Where the focus is on getting business done whatever the fallout and whoever gets hurt, there will always be the type of scandals that were discussed in Chapter 2. Controls cost money and one report on the Basel II Capital Accord response being prepared by the Bank for International Settlement suggests that British banks will have to invest around £500 million to upgrade their risk systems to comply with these new rules. Companies are resourcing the work needed to improve their internal controls and one newspaper vacancy advertisement reads:

> Internal Controls Manager for a large international business with duties being:
>
> - Co-ordinating the planning and execution of an efficient review of all key business relationships.
> - Reviewing new information system modifications prior to implementation to ensure systems integrity.

- Monitoring and reporting on the business' compliance with corporate, international and internal policies.
- Ad hoc special projects.

Another job advertisement reads:

> Director – Risk Management and Controls, responsible for:
>
> - Improving control processes across Europe, including risk management and financial systems.
> - Benchmarking and identifying opportunities to implement best practice across the group.
> - Developing the group's financial systems strategy.
> - Influencing the businesses to assume risk responsibilities.

Turnbull recognizes this link to risk and states that the board's annual assessment should consider

- the changes since the last annual assessment in the nature and extent of significant risks, and the company's ability to respond to changes in its business and the external environment;
- the scope and quality of management's ongoing monitoring of risks and of the system of internal control, and, where applicable, the work of its internal audit function and other providers of assurance;
- the extent and frequency of the communication of the results of the monitoring to the board (or board committee(s)) which enables it to build up a cumulative assessment of the state of control in the company and the effectiveness with which risk is being managed;
- the incidence of significant control failings or weaknesses that have been identified at any time during the period and the extent to which they have resulted in unforeseen outcomes or contingencies that have had, could have had, or may in the future have, a material impact on the company's financial performance or condition; and
- the effectiveness of the company's public reporting processes. (para. 33)

Changing risks call for changing controls, for example, a shift towards e-procurement may allow local managers to place orders direct with suppliers and so appear to override central buying controls. But strict criteria over suppliers, goods, prices and so on forced through the adopted information system (and associated database) can themselves act as a central buying control and so shift the control focus to automated processes with head office intervention where appropriate. The King report from South Africa makes the link between risk and controls:

> The board should make use of generally recognised risk management and internal control models and frameworks in order to maintain a sound system of risk management and internal control to provide reasonable assurance regarding the achievement of organizational objectives with respect to:
>
> - effectiveness and efficiency of operations;
> - safeguarding of the company's assets (including information);
> - compliance with applicable laws, regulations and supervisory requirements;
> - supporting business sustainability under normal as well as adverse operating conditions;
> - reliability of reporting; and behaving responsibly towards stakeholders. (para. 3.1.4)

The equation is quite simple. Controls are needed if they guard against an unacceptable risk to the business or if they are part of a legal or regulatory compliance regime. In fact, these latter controls guard against the risk of failing to comply with the regime. Controls that do not pass

these two tests may well be discarded, since they in turn cause a risk to the business by increasing costs and/or slowing down the organisation.

4.6 Control Mechanisms

Control mechanisms are all those arrangements and procedures in place to ensure the business objectives may be met. They consist of individual mechanisms used by people and processes throughout the organisation and they should exhibit certain defined attributes:

1. They should be clearly defined and understood by all users. Where a procedure is not fully appreciated by staff, there will definitely be problems associated with compliance. They should be simple to operate and make sense. So, for example, where two activities are segregated, the ensuing work should flow in a sensible way and not constitute a basic duplication of effort. They should be realistic and not too cumbersome. An office environment that relies heavily on telephone contact will stagnate if staff are asked to record in detail each phone call made and received. Rules on documentation should, in this case, take on board the level of activity that is recorded and apply only to limited instances where there is a real need to write something down. They should be regularly reviewed and amended particularly where the operation has changed. We have touched upon the control aspects of systems amendment and it is important that managers recognize this when making decisions regarding the way they organise their resources. They should be geared to the riskier aspects of the operation. This is a key factor since there is little point devising a whole series of procedures that do not relate to matters that should be of concern to management. In fact, it is most frustrating to spend time controlling areas that do not feed directly into organisational goals. Controls should be consistent in the way they are designed and applied. For example, if performance appraisal is applied to one set of staff, it makes sense to extend this to all employees where performance is a major concern. Again devolved financial management and decentralized personnel management should all relate back to corporate standards that act as a high-level control over what can and cannot be done. As such controls should not really be dependent on the individual managers but should be part of general quality standards. Furthermore, matters of fairness and equity should be a clear part of the control process across the organisation.
2. Mechanisms should be established to monitor the extent to which control is being applied in practice. Control is a process that starts with setting standards and ends with reviewing the extent to which this has been successful. Checks over the way people are using procedures are an integral part of the control process that cannot be separated from the act of installing the control features in the first place. Non-compliance is a major concern for the auditor who will seek to test this factor before accepting that suitable controls are in place. This view, however, may be challenged where we deem the review of compliance as management's role, underpinning the control process rather than relying on separate checks by the auditor.
3. Their use should be agreed by management and the staff who operate them. This factor should be used by the auditors to ensure they get managers to 'own' recommendations that impact on the systems of internal control. Suggesting that the devices that strengthen control in some way belong to the auditors creates a degree of distance between management and the control process. Managers must accept or reject a control process and this decision must be left up to them. Following this point, it is not for the managers to stand guard over their staff and ensure they do things properly. In the final analysis, we return again to the principle that control is about how people behave, and that these people are located at all levels in the

organisation. With this in mind, it is essential that the control process is driven not only by managers but also by the staff themselves.

Types of Controls

Principal controls may be categorized in a number of different ways. One way is to view them as being classified as follows:

- administrative
- informational
- managerial
- procedural
- physical.

Another way is to break them down into:

1. **Directive** – These controls ensure that there is a clear direction and drive towards achieving the stated objectives. These are positive arrangements to motivate people and give them a clear sense of direction (and the ability) to make good progress. In terms of emergency fire procedures, directive controls may consist of staff awareness training where the importance of guarding against fire, in line with a formal policy, should direct staff to mitigate the effects of this risk.
2. **Preventive** – These are controls that ensure that systems work in the first place. These may include employing competent staff, high moral standards, segregation of duties and generally establishing a good control environment. Physical and access controls such as lock, passwords and security personnel are all designed to stop people breaching the system. Banning unauthorized electrical appliances is designed to prevent fire in the first place.
3. **Detective** – These controls are designed to pick up transaction errors that have not been prevented. They cover controls such as supervisory review, internal checks, variance reporting, spot checks and reconciliations. Fire alarms are detective controls in that they will be activated in the event of a fire or release of smoke.
4. **Corrective** – The final category of controls ensures that where problems are identified they are properly dealt with. These include management action, correction and follow-up procedures. Fire appliances and fire extinguishers are designed to deal with an emergency if and when it arises, and as best as possible, correct the situation.

A combination of the above types of controls is essential to address the four key questions:

1. How do we get the right culture and drive to ensure these risks are appreciated and anticipated?
2. How do we install specific measures to prevent the risks that we now understand?
3. How can we find out if, despite our best efforts, things are still going wrong?
4. How can we plan in advance to address problems that we detect, particularly when they represent a significant risk to our business?

Many feel that a heavy dependence on detective and corrective controls may suggest an imbalance where upfront direction and prevention have not been adequately resourced.

Controls in Practice

Controls need to work well. There is one view that they should be smart, in that they should be:

- specific
- measurable
- achievable
- result oriented
- timely.

Some of the more traditional control mechanisms that may be applied in practice include:

Authorization The act of authorising something brings with it the process of granting permission on behalf of the organisation. This is normally associated with a signature from the authorising officer that records this decision. For this control to be of any use it must involve the attributes in Figure 4.7.

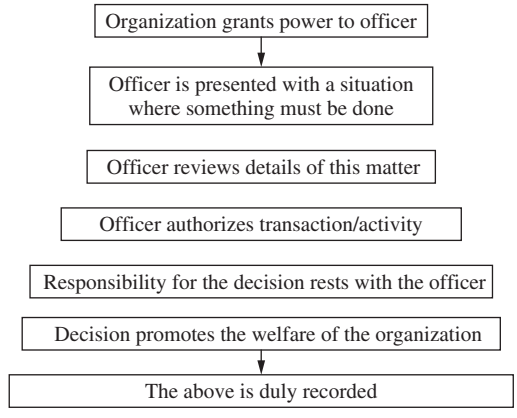


FIGURE 4.7 The exercise of authority.

Each of the above components must be fully satisfied for this control process to be relied on. Where, for example, the detail presented to the officer is false or misleading, or not properly considered, the decision may be flawed. Likewise, if the officer can disclaim responsibility for the decision then again the process breaks down. The more important the transaction, the higher the level of authority needed to approve it. Against this is the move to drive empowerment down the organisation and so the relative risk of problems such as fraud and error should be weighed against the disadvantages in passing too many items to senior management and bogging down the organisation with excessive bureaucracy. In this environment, excessive authorization routines will result in more rubber stamping, or blank forms signed or signing on behalf of someone else.

Physical access restrictions Physical access measures should be applied to information through, say, passwords, access restrictions to desktop computers and an overall policy covering buildings security. It is based on two principles. The first principle is the 'need to know/have' policy that provides information or assets only where this is necessary for the performance of one's

work. The second principle is based on the view that there is little point in leaving cash on a desk and so testing the resolve of people to resist temptation. Access restrictions only work where there is careful consideration given to the control of keys/passwords and access rights. CCTV, alarms, links with local police stations and a full-blown security policy and resource are now standard in many organisations. Where different states of alert can be defined depending on the circumstances, there can be grades of security assigned to each level. September 11 has meant a complete rethink of security arrangements, international alerts, response plans and contingency arrangements in the event of a terrorist attack. A robust response is now expected as the norm, because the risk has been seen to be real and not just perceived.

Supervision This control tends to have a dual nature whereby staff are observed first hand by their line managers, while, at the same time, these supervisors are available to help and assist their subordinates. Supervision will not really work unless these two features are firmly in place. When reviewing the success of supervision, it is not enough simply to have line managers located with their staff but we must also consider what is achieved through the relationship. Where a supervisor ignores blatant breaches of procedure (say abuse of the telephones), this impairs control.

Compliance checks We have already discussed compliance as a fundamental component of the control systems and the way it is part of the process of doing things properly. Here we consider compliance in the context of special steps taken to check on whether authorized procedures are being applied as prescribed. This is a support control that seeks independent confirmation that staff are performing in the way that was originally intended. Control teams with a remit to carry out regular compliance checks are one way of doing this. It is to be remembered that compliance checks cannot be part of a quality assurance programme unless there is an inbuilt way of tracing identified problems back to their underlying cause and so correcting them. Straightforward compliance checks simply provide a device for making sure procedures are used. A mechanism should be in place whereby the organisation is made aware of new legislation or regulations, such as changes to employment laws so that it can respond by changing its systems and ensuring compliance. It may be necessary to appoint a legal officer or an employment law or health and safety specialist.

Procedures manuals As a high level control, the organisation should set corporate standards that cover at least the following areas:

- financial regulations covering income, expenditure, cash, banking, general accounting, contracts and related matters;
- staff handbook covering recruitment, training and development, performance, discipline and so on;
- purchasing code of practice on goods and services acquired by the organisation;
- code of personal conduct with guidance on gifts and hospitality;
- computer standards on the use of computer systems and security procedures.

Where there is a limited internal audit cover to address compliance, it may be best to channel audit resources into reviewing the adequacy and effectiveness of the above-mentioned procedures as the most efficient use of audit time. Corporate procedures should be related to lower level operational procedures that set direction on matters that fall within the remit of front line officers. These more detailed procedures also constitute important control devices so long as they are

complied with. Some organisations prepare an internal control manual where some of the general control mechanisms that have been mentioned are set out, and the way they should be applied across the organisation is described.

Recruitment and staff development practices We have indicated that most controls are based around what people do and the people factor cannot be ignored. The successful operation of basic controls presupposes that the staff involved are competent, motivated, honest and alert so that they are both able and willing to perform. While much of this is dependent on good management practices based around communication and team building, the foundation is derived from using the right people in the first place. This in turn is wholly dependent on sound recruitment practices. There are many auditors who will recognize the embarrassing situation where they have completed an audit and found many problems that essentially relate back to elementary staff incompetence. It is difficult to report this matter other than as a training need. It is becoming increasingly clear that impoverished organisations, particularly in the public sector, have suffered because of inadequate recruitment procedures that lead to staff being taken on, who are not equipped to perform in any respect. Competence-led staff recruitment, training and development is an important control over the risk of poor performance among employees. An organisation that is committed to continual learning and improvements aligned to its strategic objectives has a better chance of successful growth than one that fails to resource people development. Even if teams are achieving their objectives, there is still some chance that new opportunities will be missed, resulting in long-term competitive disadvantage. A well-balanced (life/work equation) and motivated workforce, which benefits from career development, teamwork and good succession planning, will be better able to resist the risk of corporate failure.

Segregation of duties This control brings into play more than one individual during any one transaction, which can lead to an actual gain or benefit. The idea is to stop one person from undertaking a transaction from start to finish. There are obvious examples such as a payments systems where the preparation, authorization, processing and dispatching of the cheque should each be done by different people. The idea is not only to act as a check on each other's work but also to help prevent fraud. Internal check is a related procedure whereby the work of one person is checked by another so as to minimize fraud and error. As such, reliance is not placed solely on the work of one person in recognition of the human frailty that allows mistakes to occur. An example of a basic check is where staff timesheets are cross-cast by an administrative officer before being input to a time recording system. Any errors on completing this document will hopefully be thereby isolated. Segregation of duties and internal check are becoming less prevalent as we move to flatter organisations where business units have devolved responsibility for systems such as payments, income collection and payroll. The new control culture seeks rejection routines, automated audit trails and exception reports to reveal whether there has been any fraud or abuse. Where segregation of duties is poor then there would have to be compensating controls, for example, closer supervision or authorization for high value transactions.

Organisation The way an organisation is structured can promote or impair good control. Clear reporting lines that establish links between accountability, responsibility and authorization is a good start place. Sensible location of specialist staff and general managers so that the functional and line management structures complement each other rather than compete for resources is a prerequisite to good control. Organisations that flow from a robust strategy that is designed to discharge the strategic priorities with an appropriate assignment of resources, again, make for a sound platform of controls over the implementation of the set strategy. Where an organisation

has thought about the way it uses delegations and empowerment but ensures accountabilities are maintained, again controls are easier to establish. Finally, it is important that budgets are allocated in accordance with the organisational structures and that good budgetary control is applied in a flexible and practical manner. Where budgets are aligned to the decision-making processes, they will encourage better control over resources and help guard against the risk of fraud and mismanagement. Some organisations appoint an internal control officer to ensure all aspects of risk mitigation and control are addressed. There is also legislation such as the New York Government Accountability and Internal Control Act 1987 – updated in 1999 (www.osc.state.ny.us) – which details the need to establish and maintain guidelines for internal control policies, awareness and reviews for agency managers.

Sequential numbering of documents and controlled stationery Valuable documents such as orders, cheque requisitions and cheques themselves have an inbuilt control in terms of the sequential numbers. All controlled stationery should meet this criterion. The ability to check and report on these sequences creates a useful control technique where missing, duplicated or inconsistent items may be readily isolated. Transaction sequencing can be applied to many situations where we wish to monitor what is going through a system and/or what documents are being used. It is good practice to review all documents in use and decide whether there would be any benefits in having them uniquely identifiable. Any processing systems would have to record and report all irregular items for such a procedure to be of any use.

Reconciliations The act of balancing one system with another does in itself engender control. As a principle, this should be applied to all systems that have an association in terms of data from one relating to data from another. Control reports based on the reconciliations can direct management to areas where there might be problems or error. Of course, basic reconciliations also arise in accounting procedures where accounts are balanced before they are closed and posted to the final accounts. Again, the auditor may ask of any system, 'What should this balance to and does this happen in practice?' As an example, a creditors system may allow the inputter to write off a payment that has been fraudulently encashed after the cheque has been intercepted in the post, so that a fresh cheque may be raised. A separate database of fraudulently encashed cheques may also be maintained. The creditors system may then report all items coded to 'write off: fraudulent encashment', and this report should be reconciled to the fraudulent cheques database as a key control over this procedure. The list may go on and on indefinitely, since it is clear that control is about everything that management does in getting the right results.

Project and procurement management Most organisations have established ongoing change programmes to push ahead or simply keep up with the competition and heightened expectations from stakeholders. Where these programmes are supported by efficient projects based on project management principles, they have more chance of being successful. Procurement and contracting are other related areas that should be subject to the best practice standards developed by the relevant professional bodies.

Financial systems controls Most of the well-known specific controls over basic payments, income, sales, purchasing, inventory and other financial-based systems should be firmly in place. This is in spite of the move towards more devolvement of financial management to business unit managers and less head office central control. Risk tolerance for key financial systems that can be abused and defrauded should be set quite high and the corresponding controls geared into ensuring we only process the right transactions in the right manner and are able to account

for them in accordance with accounting standards and procedures. There are many well-known specific controls such as access controls, specialist finance staff, financial regulations, segregation of duties, reconciliations, exception reports, coding to budget heads, ratio analysis, retention rules on documentation, financial controller checks, external audit and so on, that help protect the financial systems and transactions.

IT security All organisations use IS and these will tend to be automated with internal networks and links to the Internet. The risks from unauthorized access, unauthorized use of data, systems crashes and poor information and reports can cause an organisation to fail altogether. An IT security policy and contingency plan should be in place and be assigned to a designated officer with links up to board level. There are numerous specific controls such as off-site documents, data encryption, automated dial back, passwords, security personnel, CCTV and data profiling that are available to tackle computer abuse. In terms of IS, COBIT provides a useful way of analysing the types of controls that may be applied:

- Application controls – These relate to the transactions and standing data appertaining to each computer-based application system and are therefore specific to each such application.
- Control risk – The risk that an error which could occur in an audit area, and which could be material, individually or in combination with other errors, will not be prevented or detected and corrected on a timely basis by the internal control system.
- Detailed IS controls – These are controls over the acquisition, implementation, delivery and support of IS systems and services. They are made up of application controls plus those general controls not included in pervasive controls.
- General controls – These are controls other than application controls, which relate to the environment within which computer-based applications are developed, maintained and operated, and which, therefore, are applicable to all the applications.
- Internal control – These are the policies, procedures and organisational structures, designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.
- Pervasive IS controls – These controls are designed to manage and monitor the IS environment and which therefore affect all IS related activities.

Performance management Another key control that should be firmly in place is related to a process whereby outputs and overall performance are examined by line management. This may involve reviewing reconciliations, working papers, reports, physical products, achievements (e.g. a new contract agreed with the client) and assessment of KPIs and so on, the point being that some form of check is made on that which staff produce. The output should be measured against a defined standard in line with the process in Figure 4.8.

This process is linked to the principle of delegation whereby staff are able to act on behalf of management, but the resultant product is still the responsibility of the same managers, who have to sign off the work done. A typical auditor's question that can be applied in almost any situation may appear as 'How do you satisfy yourself that the work has been performed to the requisite standard?' In fact, the entire performance measurement and management system will control the risk of poor performance and inefficiency. If the task of setting performance standards and measuring the extent to which KPIs are assessed is properly resourced, there will be a much better chance of operational success. Some argue that the entire control concept is based on comparing actuals with a set standard (set to ensure objectives are achieved) and that the organisation can be sure of doing the right things at the right time and cost. All important IS are geared into this process and reports help direct attention towards problems that interfere with



FIGURE 4.8 Output inspection process.

the drive to attain these set standards. The performance system should be integrated with the risk management systems and target factors critical to business success. The performance system should be:

- simple
- reliable
- accepted by all
- driven by the board
- flexible
- reflect accountabilities
- forward-looking and based on the corporate vision
- based on a clear and fair policy
- linked into the organisation's value system
- linked to objectives and their achievement
- based on a good reporting system that provides information that is timely, regular, reliable, comparable, clear (e.g. graphs) and not bogged down with excessive detail and which links clearly into personal accountabilities
- based on a learning dynamic
- tailored to the operation
- in line with the culture or be part of a culture change initiative
- responsive to changing risk management strategies
- more than anything, challenging.

The Suitability of Controls

In terms of assessing the suitability of systems of internal control, there are some danger signs that should be looked for that might lower the efficiency of the control environment.

Ability of senior management to override accepted control Many quite acceptable procedures constitute good control over staff activities so long as they are being applied. Furthermore, compliance checks may help isolate staff who do not use prescribed procedures and action can be taken to remedy this. Informal groups with decision-making powers are also able to form a pressure group that may be able to overrule control routines. Formal control

procedures that are written up and applied by all staff lead to good control. However, where there are matters that fall outside the norm, vague contingency arrangements may be in place that are, in practice, unwritten and, in part, simply made up. Where this happens, controls may break down and it may be very difficult to discover who made what decisions. The problem arises where managers are able to suspend controls at will, so as to expedite a required activity. An example follows:

> A director ruled that reception staff must check all ID cards for staff arriving at the building even where they are known. This happened for a few weeks and suddenly stopped. Reception explained, when asked why the practice had ceased, that the same director when asked to produce his ID became most annoyed and refused. Since then, it was felt that the extra checks should be abandoned.

The difficulty arises where staff feel unable to challenge senior managers who are by-passing a standard control. Where controls can be suspended for emergencies this must be agreed and written into the procedure, and ideally subject to special checks when the emergency is over.

Lack of staff and vacant posts Control relating to authorization, internal check, segregation and supervision can suffer where there are insufficient staff to enact the agreed procedure. For example, a procedure for enveloping cheques that requires two people being present is very hard to apply where there simply are not enough staff. There needs to be a level of flexibility in designing controls so that unusual circumstances, where staff are not available, may be catered to. To compensate for this, it is essential that a management trail is present that allows one to ascertain who initiated a transaction for later review and consideration. Moreover, management must assume responsibility for failing to fill vacant posts or not arranging suitable cover, thus allowing controls to be impaired. They cannot simply ignore this issue or blame it on budget restrictions.

Poor control culture The types of controls mentioned above depend on managers and staff doing things properly. It normally takes longer and can be more cumbersome to perform these control arrangements, which, in turn, takes a level of all-round discipline from staff. The aggregation of these views on discipline from all levels in the organisation constitutes what we may call the control environment or alternatively the control culture. An example follows:

> A new employee was being shown around the office and came across a book marked 'temps signing-in book'. He was surprised to find it empty despite the fact that there were several temporary staff present who had been working for many months. On making enquiries, he was told that the temps did not bother to sign in and no one insisted that they did.

Staff collusion Many controls depend on two or more staff members' involvement as a form of a check over each other's activities. The idea is that while one person could be corrupt, this would be a rare occurrence, which is catered to by not allowing an individual sole authority over one routine. This unfortunately does not take on board research that suggests many people are only as honest as controls require them to be. As such, where dishonest staff conspire to defeat controls, they can do a great deal of damage. When reviewing transactions, the fact that there are two signatures attached to a document does not mean that it is necessarily correct and proper.

In practice, there are some systems that can be wholly bypassed through well-planned collusion by key personnel.

Reliance on a single performance indicator We have agreed that controls are in place to ensure that management is able to achieve its objectives. Where these objectives are centred on performance indicators then we would expect the associated controls to recognize this factor. The problem arises where management is given one basic indicator to work to, which is regularly reported. The temptation to base one's activities around one key factor can lead to many distortions that do not necessarily promote organisational objectives. A bottom-line ratio can have unforeseen side effects that make many controls redundant as they do not contribute to the requisite figure. An example follows:

> An internal audit section had one main performance indicator, the percentage of recoverable to non-recoverable hours, which was reported to the audit committee quarterly. The committee was not interested in the achievements from the recoverable hours (i.e. reports issued) and this led to staff dumping their time to recoverable jobs. There was very little attention paid to controlling time charged to active jobs.

Reliance on memory There are some controls that are dependent on knowledge held only in the minds of employees. This may relate to identity and/or signature of authorising officers, procedures used for dealing with various activities, levels of delegated authority, key contacts, roles of respective officers and so on. While on the one hand, this gives well-deserved responsibility to long-serving employees, and, as a result, places them in a special position, it can also have many disadvantages. One is a lack of clarity as to precisely what actions the organisation has authorized. In addition, inconsistency and misunderstanding can arise where there is undue reliance placed on the discretion of the person in question. It is surprising how many systems are based on this factor that, through custom and practice, develops over time. Control is not impossible within this model but there are many dangers that can result in an overall lowering of control standards. This point can be probed by the auditor who might continue to enquire, 'What happens when this person is away? How can you be sure that this is the correct procedure?' and so on We can place reliance on memory next to the fact that long-serving and trusted employees can be involved in fraud, irregularity and basic mistakes. We move to a position where a more formalized arrangement may be required. Unfortunately, there is a socio-psychological influence that can come into play, where staff learn that it is better to operate on an informal footing in contrast to adopting formal written procedures. This is because some individuals may become almost indispensable where no one actually knows how to perform the tasks that attach to the job in question. Compiling formal documents and checklists can eventually lead to redundancy/removal for the person involved. It is therefore unfortunate that the best interests of staff do not necessarily coincide with the best interests of the organisation. Many an auditor has returned to a work area only to find that the procedures, checklists and standard documentation that he/she had previously recommended have not yet been drafted. What should be the motivation for this may be stifled by a motive that is driven by a stronger force. We return again to the question of reliance on memory and suggest that staff who seem to be muddling their way through the day in what appears to be a chaotic fashion may have actually engineered this position for their own reasons.

Retrospective transaction recording There are many managers who feel that documentation that records and/or authorizes a transaction is a matter of pure bureaucracy, which interferes

with the day-to-day running of their work area. There are times when orders are placed over the phone with the associated paperwork compiled many weeks later. There are records that are written up as and when there is time available, in many cases, the relevant detail is based mainly on memory.

Uncontrolled delegation of tasks The idea of controls is linked to various management principles that include accountability and responsibility. Having someone in charge of an operation and responsible for the end result is the best way of ensuring that there is a driving force that directs resources towards the defined goals of the organisation. This principle is fundamental to the business world as experience shows that consensus rules through various committees, blurs the decision-making process and leads to excessive bureaucracy. Responsibility does not mean that tasks cannot be delegated to various levels under a manager's command and, again, this is generally good practice. The danger lies in excessive delegation that has not been controlled in any sense. In this scenario, control suffers as staff assume responsibility for activities that should rightly be under the charge of more senior officers. It is not possible to assign tasks and walk away without checking on progress or caring about what happens. 'Scapegoating' is now a serious political issue where middle management is frequently prone to disciplinary action if a problem can be traced back to an action (or failure to act). The question of exactly who is responsible for an activity where there are problems can be key to the process of instigating such disciplinary action. Delegation can, in this respect, be a useful management tool, or a weapon to be readily abused.

Soft Controls

These are best described by Jim Roth who wrote about the importance of understanding soft controls:

> If we think our job is to evaluate compliance with policies and procedures, it leaves us nowhere. However, that's not what our organizations need. As managements move into empowerment modes, they need help with the transition. Most of all, they need us to be an independent, objective observer who will give them the kind of realistic, honest, substantial feedback that most people in the organization won't provide. So our job, I think, increasingly is going to involve evaluating these soft, intangible areas . . . In addition, all the major developments I see in internal auditing somehow relate to soft controls . . . So what do internal auditors do, other than create the audit routines? We do what helps management control an organization that is much looser, freer, and potentially more chaotic . . . To effectively evaluate the soft side of controls, auditors must demonstrate different mindsets than those of the traditional auditors. This visioning process is the right way to go about changing the auditor's mindset. Mostly, it helps the whole department focus on the specific things that need to be done. I've learned that when it comes to the softer sides of control, there is no 'one size fits all' solution. Everything has to be tailored.[15]

From our discussion so far, it should be clear that there is no such thing as an audit control. There are only management controls and, in this context, we should restate that management should establish business objectives so that for each business objective there will be underlying control objectives to ensure that the information is adequate, compliance occurs, assets are protected and value for money is promoted. Sufficient control mechanisms should be designed, installed and reviewed to ensure that these control objectives are achieved. These controls should

form a system to cover control at a corporate, managerial and operational level. We can note that internal auditors are known by many names including information systems audit, contract audit, compliance audit, fraud investigators, probity inspectors and so on. There is a view that the auditor should know more about the system under review than management and as such may tell them how best to perform their managerial duties. This is false since it is managers who must understand their areas of responsibility and audit's role is not to second-guess them. Above all, the auditor is an expert in risk and control armed with a comprehensive knowledge of control concepts. The available mechanisms and how they might be applied in practice are the main prerequisites for a professional internal auditor. The importance of a systematic approach to internal auditing has been recognized by the Basel banking committee who suggest that

> While internal audit can be an effective source of separate evaluations, it was not effective in many problem banking organisations. A combination of three factors contributed to these inadequacies: the performance of piecemeal audits, the lack of a thorough understanding of the business processes, and inadequate follow-up when problems were noted. The fragmented audit approach resulted primarily because the internal audit programs were structured as a series of discrete audits of specific activities within the same division or department, within geographic areas, or within legal entities. Because the audit process was fragmented, the business processes were not fully understood by internal audit personnel. An audit approach that would have allowed the auditors to follow processes and functions through from beginning to end (i.e., follow a single transaction through from the point of transaction initiation to financial reporting phase) would have enabled them to gain a better understanding. Moreover, it would have provided the opportunity to verify and test the adequacy of controls at every step of the process. (para. 13)

4.7 Importance of Procedures

The previous section on control mechanisms outlined the different types of controls that are available when designing a suitable system of controls. As such, we can now refine our control model in Figure 4.9 to incorporate the additional features that have been described.

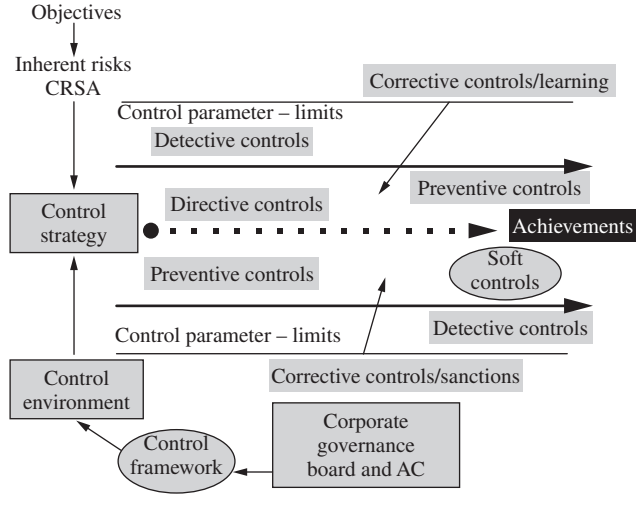


FIGURE 4.9 Internal control (5).

The preventive controls were already on our model and they revolve around the upper and lower control parameters, above and below the achievements line. We then set additional levels outside the two parameters and locate detective controls outside the control parameters. These detective controls will pick up transactions and activity that fall outside the acceptable limits (parameters) or appear likely to go outside these limits. The detective controls will tend to be information-based and will ring alarms when management intervention is needed to deal with activity that either has gone or appears to be going haywire. Corrective controls, as we have discussed, are measures designed to put right any deviations that have been detected and hence the arrowed lines start at the corrective control and then go back inside the control parameters. The final addition is soft controls that focus on the hearts and minds of people to encourage them to take responsibility for their controls and to take action where appropriate. There is a complicated view of control and a more simple version. The complicated view is based around our control model and recognizes the wide variety and range of controls that can be applied to getting the job done. The simple view is that most risks to operations can be mitigated through better procedures, that is, ways of doing the job. Hence, the importance of good procedures as a major arm of the risk management strategy. We can base our discussion of procedures around an amended version of a model (in Figure 4.10) first used in the book *Internal Control: A Manager's Journey*.[16]

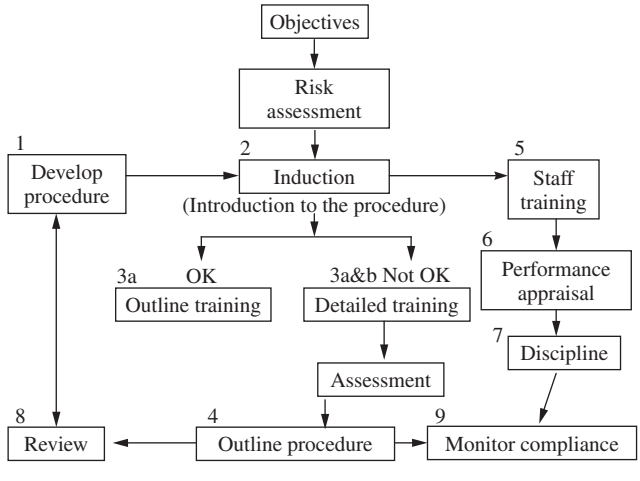


FIGURE 4.10 Implementing procedures.

Once the operational risk assessment has identified the need for tighter procedures, the task is then set to make and issue an improved version for staff. By going through the nine-stage model, there is a better change to get procedures correct, understood and accepted in the operation in question. Taking each stage of the model in turn:

1. **Development** – This involves reviewing the underlying processes, simplifying them and working with users – then drafting an agreed document that reflects the required activities.
2. **Induction** – It is important to introduce the procedure to new starters and show existing staff a new or improved procedure.
3. **The training manual** – This may be broken down into two levels. Where staff are assessed as able to apply procedures, an outline manual ('a') can be provided. Where this is not the

case, a more comprehensive package ('a&b') with exercises can be given to them to work through.

4. **Outline** – After the training or induction period, it is possible to turn to a short-cut outline document with key tasks and processes summarized for use thereafter.
5. **Training** – The skills of staff affect the degree to which procedures are successful. The training on procedures is mainly about knowledge and to supplement this, we should also seek to develop the underlying skills and the appropriate attitudes as a parallel training initiative.
6. **Appraisal** – This links the way staff are using procedures in their performance appraisal framework. In this way, it is seen to have some meaning for the work people do and their individual development programmes.
7. **Discipline** – This is a fall-back position, where, if all else fails, staff may need to be disciplined for breach of procedure.
8. **The review process** – This should be straightforward in that it entails keeping the procedure relevant, vibrant and up to date.
9. **Compliance** – This stage deals with compliance and it is the line manager's responsibility to ensure staff comply with procedure. This is best done by getting staff to understand how they can monitor themselves, and supporting them in this task.

There is a lot to the simple view of better control, which is based on better procedures. Because procedures are so important to the business it is worthwhile resourcing efforts to get them focused on known risks and integrated into the way people work.

4.8 Integrating Controls

The control model comes back into the frame with a few additional features covering performance, communications, and policy, competence and training as in Figure 4.11.

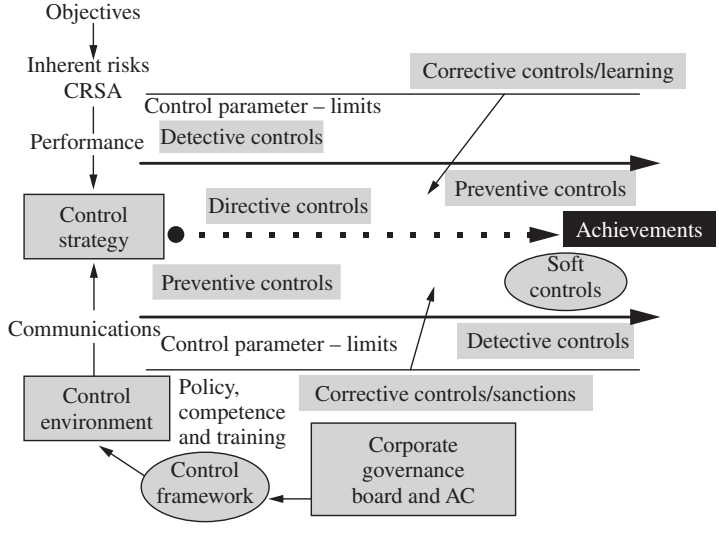


FIGURE 4.11 Internal control (6).

Each of these is now explained.

Performance The process of assessing risk must fit and be integrated with the performance management system. Dealing with risk properly is part of good management and should therefore be a task that is measured along with other obligations for managers and teams throughout the organisation. Any other way of viewing risk activities is rather pointless. As such, the control strategy that is applied to dealing with known and anticipated risks to our current and future plans is, in turn, aligned to the performance system that is in place for all operational areas and support services. This is the start to integrating controls into the work ethos. Where the strategic direction and controls are out of alignment, there will be conflicting forces that make business life difficult as described by Tony Hope and Jeremy Hope:

> But in many organizations the strategic direction and budgeting systems are contradictory. Budgets invariably mirror the historical organizational structure of the firm, so their focus is on the performance of functions, departments, cost centres and divisions. Managers are measured on their own piece of the hierarchy rather than on their contribution to strategic objectives; and this divergence is reinforced by reward and recognition systems. It is easy to see why the budgeting ethos is the antithesis of radical change. A percentage change from last year is the norm, with weeks of mindless negotiation along the way. What is the incentive of presenting high-risk strategies based on revolutionary thinking when planning for a 10 per cent cost cut here and a 15 per cent sales increase there meets expectations. Such an approach is the ultimate in managerial myopia.[17]

Communications The control model is improved by the addition of good communications in the organisation. This factor fits between the control environment and the adopted control strategy, but is also important through all aspects of the model. Communication is the main way of achieving assent from all the players in the operation and is a key consideration when devising control solutions. Poorly controlled organisations are normally held back by poor communications. And it is the control policy that is most important to bring to employees at whatever level they operate. In fact, excessive controls can slow down communications as demonstrated by David MaNamee and Georges Selim:

> When controls are the central theme of the internal audit, more and more audit reports and recommendations are generated for improving and strengthening internal controls. Over time, layer and layer of controls are built up, creating a type of 'organizational plaque'. These excessive layers of control slow down business processes. Communication becomes more difficult, and too many people are employed in non-value-adding work. Drastic measures are usually necessary to remove the built-up layers of excessive control.[18]

Policy, competence and training The crucial pivot for the control model is the Policy on Internal Control. This sets standards, roles and key messages on what internal control means and what mechanisms are available to help promote good control and so turn aspirations into achievements. The control policy may be located in the risk policy as a component within the overall risk assessment and management regime. The next item to note is the links to competence, that is that employees should have an understanding of internal controls and the ability to recognize and apply suitable techniques and mechanisms to address unacceptable risks. Having the right staff competencies (i.e. knowledge, skills and attitudes) is a useful start to getting proficient internal controls in place. After this, training and development are required to ensure the set competencies are obtained and applied to the workplace. Induction training and refresher courses and ongoing

advanced seminars can all be used to bring home the message that everyone is responsible for ensuring control and that suitable internal controls need to be in place to discharge fiduciary obligations to the organisation's stakeholders. Extracts from the NASA Policy Directive on Internal Management Controls shows how clear statements can be made to drive home the key messages:

> NASA management will establish controls to provide a reasonable assurance of the following:
>
> - Managed activities achieve their intended results.
> - Management activities are protected from waste, fraud, unauthorised use, misappropriation, and mismanagement.
> - Resources are used consistent with NASA mission.
> - Laws and regulations are followed.
> - Reliable and timely information is obtained, maintained, reported, and used for decision making.
>
> All NASA managers will periodically evaluate the effectiveness of their management controls.[19]

One further point is to reconsider the corrective controls that have appeared in the control model. The upper version has an add-on (learning) which suggests that people need to learn from their experiences where controls have failed, or they do not respond to changes in risk profiles or there have been near-misses that suggest a problem. This ongoing learning and improvement is based on the assumption that most problems experienced by an organisation can be traced to a failing in control of sorts. The lower version of corrective controls in the model has a different add-on (sanctions) that suggests that corrective controls that address a failing of directive or preventive controls may be the result of breach of procedure and/or negligence by one or more employees. Here an organisation must be firm and determine whether control failure is a learning opportunity or the result of outright staff misconduct. This factor must be built into the control model to deal with those rare circumstances where people have failed to live up to the standards expected from them with no reasonable excuse. Sanctions may include warning, demotion and transfers, as well as, ultimately, dismissal. If sanctions are used as a first resort and are the norm in dealing with avoidable control failure, there is likely to be a blame culture in place and the control model will be seen by most employees as an enforced constraint that creates stress, tension and unfair practices, which is the opposite to what the model is seeking to achieve. If, on the other hand, the control model acts as a corporate interpretation of the means to manage risk and ensure the business is successful, it reverts to the positive footing for control that it is intended to be.

4.9 The Fallacy of Perfection

There is a great deal of material around on internal control. Any Internet search on 'internal controls' will bring up hundreds if not thousands of individual devices (control mechanisms) that relate to many of the key business systems like procurement, income, transport, stores and so on. The searcher may take the view that anything and everything can be controlled with the right set of measures and this position leads us to the fallacy of perfection. The more measures put in place to achieve objectives, the better the chances of success. Or, put in another way, the greater the uncertainty of achieving objectives, the more measures are needed to reduce this uncertainty. But the measures will normally cost money and time and will tend to involve doing more work,

to get to the end result. In business, time, additional work and cost are all factors that run counter to success, in that most organisations try to generate business quickly, cheaply and with the least effort. So control measures may appear to run counter to business success but at the same time, many of these control measures are needed give the organisation its best chance of achieving success. To sum up, it may be suggested that:

- controls tend to cost money and slow an organisation down;
- controls are needed to help manage risks to an organisation's business;
- controls cannot guarantee success;
- control is effected through people and dependent on the way they behave and relate to each other;
- even the best-managed organisation can fail.

The fallacy is that controls will ensure success and it is just a question of how many measures are needed and how they should be best implemented. Against these unrealistic expectations, the COSO website makes it clear what internal control cannot do by examining some of the common myths:

- Internal control can ensure an entity's success – that is, it will ensure achievement of basic business objectives or will, at the least, ensure survival. Even effective internal control can only help an entity achieve these objectives. It can provide management information about the entity's progress, or lack of it, toward their achievement. But internal control cannot change an inherently poor manager into a good one. And, shifts in government policy or programs, competitors' actions or economic conditions can be beyond management's control. Internal control cannot ensure success, or even survival.
- Internal control can ensure the reliability of financial reporting and compliance with laws and regulations. This belief is also unwarranted. An internal control system, no matter how well conceived and operated, can provide only reasonable – not absolute – assurance to management and the board regarding achievement of an entity's objectives. The likelihood of achievement is affected by limitations inherent in all internal control systems. These include the realities that judgments in decision-making can be faulty, and that breakdowns can occur because of simple error or mistake. Additionally, controls can be circumvented by the collusion of two or more people, and management has the ability to override the system. Another limiting factor is that the design of an internal control system must reflect the fact that there are resource constraints, and the benefits of controls must be considered relative to their costs.

Thus, while internal control can help an entity achieve its objectives, it is not a panacea. Turning to the UK, Turnbull has reinforced this point:

> A sound system of internal control reduces, but cannot eliminate, the possibility of poor judgement in decision-making; human error; control processes being deliberately circumvented by employees and others; management overriding controls; and the occurrence of unforeseeable circumstances. (para. 23). A sound system of internal control therefore provides reasonable, but not absolute, assurance that a company will not be hindered in achieving its business objectives, or in the orderly and legitimate conduct of its business, by circumstances which may reasonably be foreseen. A system of internal control cannot, however, provide protection with certainty against a company failing to meet its business objectives or all material errors, losses, fraud, or breaches of laws or regulations. (para. 24)

This is a fundamental point that runs across the whole concept of risk management. The extent to which controls should guard against risks depends on the risk appetite of the organisation and its managers. In some parts of an organisation (say marketing and communications), risk seeking is rewarded, while in others (say finance and production), it is frowned on. In some parts of an organisation, people are encouraged to go ahead and try out new approaches to their business while in others, the adage 'just repeat what we did last year' rules and basic routine is the norm. Moreover, where there is ownership of the controls by the work teams, there is more chance of a positive environment that helps drive the organisation forward. While overcontrol tends to slow an organisation down, Sawyer has issued a warning about the effects of overcontrol:

> One fear that followed passage of the U.S. Foreign Corrupt Practices Act of 1977 was the possibility of excessive, redundant, useless, and/or inordinately expensive controls. When a difficulty arises, the tendency sometimes is to throw money at it and hope that it will subside. But too much control can be as bad as too little. Expensive, restrictive controls can stifle performance and initiative. Protection is bought at the price of repression.[20]

The empowerment concept that is the rallying call for most large organisations has changed the perception of controls and the self-control concept is growing as the norm in developing better and more focused controls. Note that control risk self-assessment (CSA) is dealt with in separate sections of the Handbook. Here we need to note the benefits of getting people to own their controls by examining Figure 4.12 borrowed from *Internal Control: A Manager's Journey*.[21]

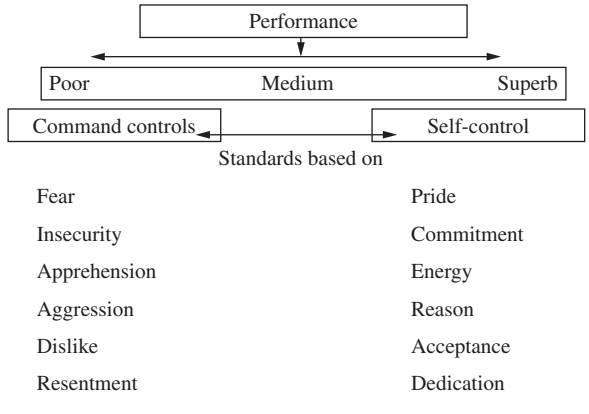


FIGURE 4.12 Controls and performance.

The left-hand side of the model features the rather negative control culture that derives from a traditional command and control approach. Meanwhile, the right-hand side indicates the result of a self-control environment where ownership promotes a more positive and forward-looking culture. The suggestion is that positive control cultures create better performance than the negative version as risks are managed in the way that makes sense to the people at a grassroots level. So long as there is an acceptance that controls cannot be relied on for absolute assurance of success, they allow for discretion and some failures, and so will make more sense to everyone. This equation does, however, depend on congruence on risk tolerance within the organisation, even if there are different degrees of tolerance for different types of risk.

4.10 Internal Control Awareness Training

If everyone had a clear understanding of internal controls and they were motivated to establish good controls in line with risk-assessed operations and functions within an organisation, then controls are more likely to work. Staff awareness training is one way of getting the message across the organisation, and is often missed out of the CRSA exercises that are now becoming popular. We can refer to the final version of our control model and use this as the basis for awareness seminars. The final version appears in Figure 4.13.

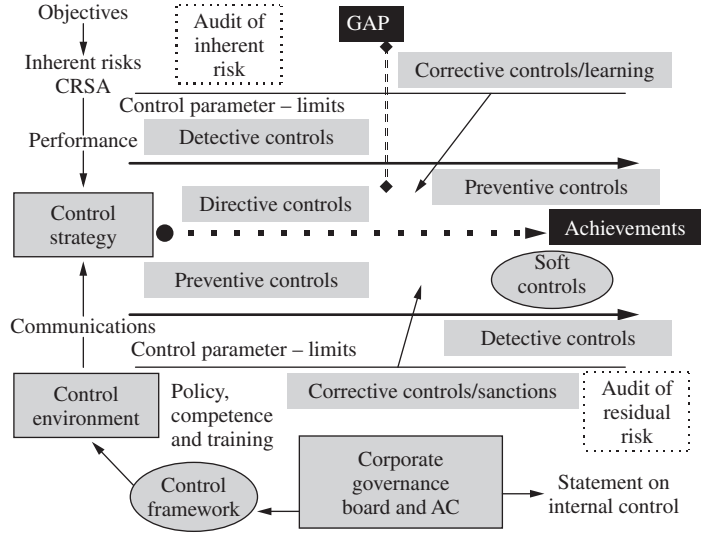


FIGURE 4.13 Internal control (7).

The additional items to complete the model are described.

Audit of inherent risk Superimposed on the control model is the role of internal audit and external audit. External audit will want to see that the underlying financial systems and accounting policies applied do not lead to any material misstatement of the financial accounts. They will also want to see that there is no fraud or non-compliance that has a material impact on the accounts. Their audit tests will provide a reasonable expectation that these types of inherent risks are not present and much hinges on the definition of material and the reliance placed on published financial statements by various users. Internal audit will want to help management deal with inherent risk in a professional manner by providing advice and consulting input to management's efforts to deal with business risk.

Audit of residual risk Internal audit will also be concerned that the risks that remain after controls have been applied are fully understood and acceptable. The focus on residual risk needs an audit approach that drills down in the way controls are working in practice and considers evidence that either supports or challenges this view. This mainly revolves around internal audit's assurance role. Since residual risk is that which remains after controls are put in place, the scale of this risk depends on the success of the control regime, which may not always be what it appears as one article demonstrates:

> Desperate health chiefs 'hid' seriously ill patients waiting for admission to hospital to try to distort a survey of the NHS, it was claimed yesterday. Senior nurses were 'pressured' into clearing out accident and emergency departments just hours before a spot-check across England and Wales. In one instance, a ward was re-opened at the last minute. At another hospital, patients waiting in casualty were distributed around the building and 'placed in beds irrespective of needs'.[22]

Statement of internal control One important constituent of the control model is the feed into the published statement on internal control. Turnbull makes it clear that the board should report on its internal controls:

> The board should define the process to be adopted for its review of the effectiveness of internal control. This should encompass both the scope and frequency of the reports it receives and reviews during the year, and also the process for its annual assessment, such that it will be provided with sound, appropriately documented, support for its statement on internal control in the company's annual report and accounts. (para. 29)

Gap The final part of the control model consists of a single 'gap' that breaks through the upper and lower control parameters. This gap may be defined as 'an extra capacity to allow for growth and the potential to reach outside the norm, challenge existing assumptions and search for new corporate inspiration'. This is important so that control frameworks don't just contain activities, but also allow for some experimentation and innovation that break the rules but still sit within the constitution. An enterprise may give someone a budget and tell them to go away for a month and come back with new ideas, in any way they deem appropriate. This person may be allowed to break the normal project management rules, so long as the person stays within the spirit of the overall value system. The concept of innovation has been explored by Barry Quirk:

> Innovation is the source of enhanced operational effectiveness. In large organizations, it needs nurturing and encouragement. But we know that the majority of innovations do not lead to progress. In fact, we only achieve progress through a proper understanding of our errors. But error has few friends in the public sector. For there is a sophisticated six-syllable word, 'accountability' that is so easily compressed in a shorter and cruder word – 'blame'. This is unfortunate, for the essence of progressive organisations is their ability to learn critically from their mistakes and errors. The public sector needs to develop a better understanding of risktaking (what sorts of risks should a public servant be encouraged to take with the public's money and what risks should be avoid). And it needs to better approach to promoting innovation, entrepreneurship and system-wide knowledge sharing.[23]

This gap may be crucial to survival. There are many who see the business of the future revolving around the Internet, where instead of selling to customers, the tables are turned and the customer simply sets out what they need (a personal specification) and sends this proposal to their favourite suppliers and waits to see which one provides the best, cheapest and quickest response. Flexibility and responsiveness become the bywords for future business success and controls that stop this from happening will have to be discarded, that is, there has to be a gap in control constraints that allows such versatility. Now that the control model is complete, we can turn to staff control awareness seminars. These seminars should be designed to suit the organisation and needs of the employees. One example of such a design is noted below for reference, and involves working through the following main stages:

1. Identify a board sponsor for the training and ensure they endorse the objectives and monitor the way such training is delivered.
2. Set a clear purpose for the awareness programme such as 'to provide participants with an awareness of the corporate policy on internal control and an understanding of their responsibilities for managing risk'. If there is no such corporate policy it may be an idea to suggest one is established before the training programme is developed.
3. Make sure each group is organised in a sensible manner that means each of the members will benefit from being at the same training event.
4. Send out pre-course material that explains the purpose of the programme including the internal control policy and ask them to identify one thing they like about the policy and one thing they do not. This pre-course material may be posted on the corporate intranet.
5. Start the event with a key note message from the board member (or most senior person around at the time), indicating why they are here and why this is important to the future success of the organisation.
6. Welcome the participants and introduce the event. Ask each participant for their name, section, role and what they liked and did not like about the internal control policy. Write the points up in front of the group. This provides a good indication on the knowledge level of the group and their general attitude towards the subject. The information may be asked for beforehand although return rates tend to be poor.
7. Introduce yourself and tell them why you think this programme is important. The group will feed off your energies.
8. Go through the day's sessions and make it clear that it is interactive and you welcome input from each person present.
9. Reinforce this point by asking the group to work in pairs for ten minutes to identify the benefits of having sound and sensible systems of internal control. Ask each pair for a benefit and write them up. Go through them at the end and add some others to form a positive basis for the event. The group may produce items such as 'makes sure right things are done'; 'checks figures'; 'stops fraud'; 'creates consistency'; and so on. Provide a formal definition of internal control at the close of this exercise and write up the objectives, inherent risks, controls and residual risk model and make it clear that there is always a chance that controls will fail and objectives will not be met. Allude to the concept of risk appetite when discussing residual risk.
10. Tell the group to settle down to a presentation and that they can interrupt whenever they wish. Promise the group that they will have mastered the entire model (from this chapter) by the end of the day. Give out a laminated version of the model with their names on their copy. Reinforce the view that training must be challenging to be of any use. A presentation pack can be given out containing each component of the model with accompanying notes with space for further notes.
11. There could be time for a coffee break at this stage.
12. Start with the Corporate Governance box of our model and explain the agency theory where board and managers are entrusted to run the business on behalf of shareholders, stakeholders and the customers. Also that the organisation has to stay within the law and regulations and ethical values that it sets (and is expected to set). Ask the group to develop a list of stakeholders.
13. Suggest that the company (or organisation) needs to make a public statement on internal control (SIC), which says there are suitable controls in place that give a reasonable expectation that objectives will be achieved (by managing the risks that stop this achievement).

14. Go to the Control Framework box and explain COSO and CoCo or the framework adopted by the organisation. The control model being used here can be said to be a control framework of sorts.
15. Go to the Control Environment box and explain that this forms the basis for the system of controls. Ask the group to assess the control environment in their section using a simple checklist of questions. Reinforce the importance of ethical values.
16. Mention that Policy, Competence and Training come in here and that this event is part of the training provision. Ask participants to list what they should know about controls to meet the competence requirements. This should be a light-hearted exercise that can be played for a few laughs.
17. Switch to the top of the model and go through the objectives, inherent risks and the adopted control strategy. Make it clear that controls are measures to ensure greater certainty that objectives will be met. Get the group to identify some of the inherent risks in their operational area and write them up. All the feedback from the group that is written up should be on show and referred to when relevant (e.g. benefits of internal control). The model in Figure 4.14 may be used to explain the objectives, risks, and controls process.



FIGURE 4.14 Risk and control cycle.

18. Explain how this risk assessment leads to a focused control strategy. For some of the risks identified by the group, ask for a vote on Impact and Probability and for more significant risks ask them to define a good control strategy. At this stage, introduce the concept of a risk register. Suggest to the group that we need to self-assess our controls as this is part of our team responsibilities. Internal audit can help with this requirement and can also check that it is being done properly but they cannot take responsibility for operational controls.
19. There could be a lunch break at this stage.
20. Go into internal control proper and start with the control parameters where teams work towards their targets (Achievements) but need to keep within the upper and lower limits. Directive controls ensure this drive from where we are to where we need to be. For buying decisions, a clear purchasing policy and procedure will act as a directive control over this activity.
21. Explain preventive controls that keep up within the two limits. A system that means only vetted suppliers can be used for significant purchases helps to address the risk of placing orders with people who are not viable.

22. Explain detective controls that ensure problems are rectified. Mention the learning concept and also the sanction concept to ensure compliance. Random checks on local orders placed by business unit managers may isolate breaches of the purchasing procedure. It may be that the manager did not understand the procedure and there is a learning opportunity. Or it may be that the orders were placed in a negligent and even suspicious manner, which may require sanctions. Tell the group that they need to think about ensuring compliance with key controls. Key controls are those specific arrangements that, if not in place, will make a system significantly vulnerable. For buying systems, the need for an approved order for material items acts as a key control over the risk of abuse, fraud, error and waste. Mention that compensating controls can be applied where a standard control does not work well and other arrangements are used to cover any deficiencies. Compensating controls should really be considered to assess whether they should officially replace documented controls. Ask the group to speak about any extra measures they take to make up for gaps in the official procedure – these are compensating controls.
23. Suggest that, together, these different types of controls form a control strategy. Mention some of the common hard controls such as separation of duties, authorization, organisation, supervision, reconciliation, documentation, physical counts, performance targets and so on.
24. Tell the group about a triangular model of Cost, Time and Quality where objectives may need to balance these three competing forces. The control system needs to be flexed to fit the set priorities – is it most important to do things quickly, or cheaply or to the highest standards, and how are these inherent conflicts perceived? It is difficult to achieve all three ideals at the same time – there tends to be some give. An example may be to ensure group members arrive at this training event on time and in a good state of mind. One solution may be to book into a nearby hotel. This ensures arrival on time and without the hassle of travelling, but it is expensive and means less time at home. Each option has a different effect on the time, cost and quality factors.
25. Work on a full-blown exercise using subgroups. The groups will need a clear task to illustrate the principles in hand. These can be work-related in that they review their risks and control, although this will take some time. Or it can be non-work-related just to illustrate the points raised. One example is taken from the book *Internal Control: A Manager's Journey*, where the task is to go abroad to the Caribbean on holiday and, while there, bring back a box of top-quality mangoes (for a favourite uncle). The objectives, risks and controls may end up in a risk register similar to the one used in our example in Table 4.1.

    If the risk management strategy is interfaced with planning, performance and decision-making and responsibility is assigned to the risk (or process) owner, then the register becomes more useful. Moreover, if an assessment process is included that monitors that the required action has been effected (perhaps through KPIs) then we arrive at a dynamic and reliable self-assessed register.
26. Work through the idea of different types of controls. Directive control: a procedure for buying items on holiday recommended by a family friend. Preventive control: a fixed amount of funds to buy mangoes to avoid overspends. Detective control: a local guide who checks the mangoes that are bought for quality. Corrective control: reporting aggressive hassling by vendors to the local hotels who will try to recover any money wasted on bad purchases.
27. Explain how the entire control system comes together in a risk management strategy where some risks may be accepted, such as taking too much time to find the mangoes, as the holiday means time is not a problem and there is an abundance of fruit available. What is more, the risk strategy increases the chances of success, but in the event that there are problems in

TABLE 4.1 Internal control evaluation.

System objective: Buying mangoes
Control objectives: Reasonable price; Good quality (undamaged); Without too much delay; Without too much hassle

Control objective	*Risks*	*Impact H M L (3) (2) (1) *A*	*Likely with no controls (0–1) *B*	*Risks managed (score) *C*
Reasonable price	price inflated artificially	**M (2)** prices are low anyway	**0.5** buyer looks like a tourist	**(1.0)** not a big issue. Get an idea of usual price range and then haggle
Good quality (undamaged)	fruit appears good but is of poor quality	**H (3)** uncle will complain	**0.9** past experience of poor fruit	**(2.7)** major risk. Need outside expertise from a local person
Without too much delay	good fruit hard to find	**L (1)** no real time pressure	**0.2** mangoes not hard to find	**(0.2)** accept this low level risk
Without too much hassle	unpleasant arguments over price	**M (2)** supposed to be a vacation	**0.3** most vendors are pleasant	**(0.6)** avoid certain traders, e.g. from isolated side roads

(* $A \times B = C$)

achieving the agreed objective, we can point to our efforts to succeed and seek to amend the risk strategy in a positive way, rather than simply blame each other for any failures.

28. Present the concept of soft controls covering, for example, the way we see the value of the set task and the extent to which our commitment and energies can be harnessed to better effect. Find out from the group what aspects of operational controls motivate them and which aspects frustrate them.
29. Go though the audit role for inherent risk from the control model and the audit role for the residual risk. Talk some more about risk appetite and whether residual risk is acceptable or not and how we need to install measures to determine whether controls work and are complied with. Ask the group for examples of large residual risk (to achieving objectives) in their work areas and instances where risk appetite has been communicated (or indeed not properly communicated) by senior management or stakeholders. A simple example may be used to illustrate risk appetite, say whether you check the weather forecast each day, to help you decide whether to carry an umbrella, or just do not bother.
30. Deal with two other aspects of the model – Communication and Performance, Management – to introduce the idea of integrating the control strategy with the way the organisation works and assesses its performance.
31. Ask the group to suggest what the final GAP (black box in Figure 4.13) is about. Put them into groups of three and start a quiz where they may ask you one question (for a tip) and then make a guess. Award a prize (an apple?) to the group that gets the closest answer. The group must first answer a simple question to get a tip and then have one guess at the answer. The simple questions are based on points already made during the day regarding internal

control and the corporate internal control policy. This also represents a way of testing the learning progress made by the group.

32. Make clear that the GAP (in Figure 4.13) is about innovation and freedom to explore assumptions. Ask the group for suggestions for improving innovation and then relate the responses to the way controls can be kept flexible and empowering, while still retaining accountability, integrity and transparency.
33. Return to the benefits of internal control that the group developed at the start of the event and reinforce some of the positive points raised. Tell the group that designing controls to mitigate risk is not an easy task and all controls should be worth the effort. So it is only worthwhile having 24-hour security for the head office building if there is a risk that warrants night-time as well as daytime security cover. Give the group (in pairs) ten minutes to do a final exercise – to prepare a list of attributes of good controls. Go round the room and ask each pair to shout out their attribute and list write each one on a flip chart (or powerbeam). The group will come up with ideas such as simple, flexible, clear, accepted by people, communicated, understood, fits culture, promotes integrity, leads to desired results, makes good common sense, is cost effective, does not slow things down too much, promotes teamworking, reflects authority levels, customer friendly, documented, changed when redundant, used consistently, not overly technical, fits values, not too easily abused, measurable, consistent with KPIs, allows some discretion, stops excessive discretion, promotes sound judgements – and so on. Tell the group that these points provide criteria to measure the value of proposed controls and where possible each new control should be assessed against similar criteria before it is adopted. There are some risks that we have to accept because it is too difficult to guard against them and still run the business; controls are not necessarily panaceas; it is never as simple as that. Remember the three factors – integrity, transparency and accountability – if we can deliver the business and achieve the three factors, and apply good common sense, then we will have some control over our work.
34. Summarize the day's work and go back to the control model and ask each person to briefly discuss one aspect of the model. Keep it light and move on when someone gets stuck and encourage everyone to make an input.
35. Go back to the event's original aim and keynote message given at the start.
36. Suggest ways that the participants will use the event to review their controls and point to any CRSA programmes that are available, as well as material on the intranet and where to go to for further advice.
37. Ask each participant to name one thing they have gained from the day and close on a positive note.
38. Get each person to fill in a feedback form and invite further comments that can be sent in later. Ask participants to give further feedback after three months which indicates ways that the event has contributed to their performance.
39. Dismiss the group and privately pick on the two most sensible people present to stay back and ask their view of the event and what they liked and what can be improved.
40. Report results back to the board programme sponsor.
41. Redesign the event where required.

The training may be multimedia based where the learning points are achieved through interactive session through the corporate intranet. Or it may be possible for people to work in small teams of twos or threes, taking turns to use the computer interface. The best impact method is through actual seminars/workshops wherever possible. Also two presenters (or facilitators) will provide better results if the resources are available. The starting place for this type of activity involves several main drivers:

- a corporate policy on risk and internal control;
- the board's involvement;
- staff competencies that include a good understanding of internal control concepts, design and review;
- a resource (trainer) that is able to lead the training event;
- a commitment to sound controls that means time is found for training programmes.

If these forces are in place, then there is a good chance that an organisation may empower its people to take responsibility for ensuring there are good systems of internal control both protecting and promoting the business.

4.11 New Developments

In most developed countries, the system of internal control has to be reviewed in listed companies as part of regulatory provisions. Regulatory codes can get quite complex but a simple way of viewing the controls oversight concept is set out below:

- The board sets the policy on internal control on behalf of their shareholders and oversee the results, with help from their audit committee.
- Management implement this policy to ensure the business is properly controlled. In fact, the new perspective is that management itself will want to ensure controls work and that their staff can give them assurances that controls are in place and adhered to.
- Various compliance, risk, financial control and internal performance and assurance teams will each contribute to the pool of knowledge on the state of controls and where they need to be improved.
- Internal audit review controls and provide independent assurances to the management and the audit committee. Under their consulting arm, the internal auditor may well help improve risk management processes and specific controls.
- External audit assess key controls over the financial reporting system to reduce the amount of testing they need to carry to form an opinion on the accounts. Besides carrying out testing routines, external audit are starting to form opinions on the adequacy of financial controls as part of the overall system of internal control.
- The board report on their arrangements to ensure sound controls, which depends on an effective risk management process.
- The shareholders will need to satisfy themselves that the above arrangements work, and one way is to consider the views of the audit committee.

The Financial Reporting Council explained the current controls disclosure requirements and the effect of the 2006 Companies Act:

> Section C.2 of the Combined Code states that companies should maintain a sound system of internal control, the effectiveness of which should be reviewed at least annually with the review being reported on in the annual report. Further guidance on this subject, including recommendations on disclosure, is set out in the Turnbull Guidance, which was last revised in 2005.
>
> Listed companies are also required under the Companies Act 2006 to include in the Business Review a description of the principal risks and uncertainties facing the company, and under the

FSA's Disclosure and Transparency Rules to describe the main features of the internal control system as it relates to financial reporting. In addition, IFRS 7 requires companies to set out in their audited accounts how they manage financial risks and a summary of the information that key operating decision makers use to manage those risks. All of these disclosures are monitored by the Financial Reporting Review Panel (FRRP), which is part of the FRC.

Many commentators on the review distinguished between the management of operational risks, for which the majority considered existing processes and guidance to be sufficient (at least for non-financial companies), and the management of strategic risks, in particular "high impact, low probability" risks. In the latter case the board's responsibility for setting the risk appetite and profile of the company was of particular importance. There was a view that not all boards had carried out this role adequately, and in discussion with the chairmen of listed companies many agreed that the financial crisis had led their boards to devote more time to consideration of the major risks facing the company. There were differing views about the extent to which risk management systems below board level may need to be reviewed in non-financial companies. Some commentators on the review were critical of companies' reporting on risk, which investors felt was often uninformative. In its most recent annual review, published in October 20087, the FRRP also identified some common failings in business reviews including lack of clarity about the business model and specific risks and uncertainties, and the use of boiler-plate descriptions. As noted above there are various overlapping disclosure requirements relating to risk management and internal controls, and this complexity adds to the difficulty for both companies and readers of annual reports. It may be possible to rationalise these requirements, although the scope for doing so is constrained by the fact that many of them are required by statute or FSA Rules.[22]

One development occurred in 2008, when COSO released a document, Guidance on Monitoring Internal Control Systems, to help organisations monitor the quality of their internal control systems. Eddie Best has provided an outline of this guidance. The new COSO guidance provides broad direction to help:

- Identify and leverage good monitoring practices
- Reduce redundancies
- Recognise inefficiencies and weaknesses
- Embed effective monitoring into everyday practices

Here are the three steps:

1. **Establish a foundation**: Is monitoring currently a priority in your organisation? Set a tone from the top that conveys the importance of monitoring. Consider the roles of management and the board with respect to monitoring and the use of evaluators. Identify who oversees which areas of control and any potential impairment of objectivity. Ensure that your organisation has a baseline understanding of your internal control system's effectiveness.
2. **Design and execute**: The crux of monitoring is designing and executing procedures that evaluate important controls over meaningful risks.
   - **Prioritise risks**: Understand and prioritise risks to organisational objectives
   - **Identify controls**: Identify key controls that address those prioritised risks
   - **Identify information**: Identify information that will persuasively indicate whether the internal control system is operating effectively
   - **Implement monitoring**: Develop and implement cost-effective procedures to evaluate that persuasive information. Choose the right information for the given circumstances
3. **Assess and report**: The final step is assessing and reporting results. Prioritise deficiencies by significance and the likelihood a deficiency will result in an error, giving due consideration

> to the effectiveness of other compensating controls. By evaluating your internal control system in this way, deficiencies can be identified and addressed before they materially affect the organisation. Management, the board and internal auditors all play important roles in the monitoring process and should take a proactive approach in its implementation.
>
> The ultimate efficacy of this guidance, as with many aspects of effective management, hinges on sound judgment. Integrating the objective examination of monitoring processes and preventative measures being exercised into organisational management will promote successful delivery of strategic objectives.[24]

It is possible to place internal controls at the forefront of governance, and this view is helped by guidance from the Centre for Financial Market Integrity:

> Corporate governance is the system of internal controls and procedures by which individual companies are managed. It provides a framework that defines the rights, roles, and responsibilities of various groups – management, board, controlling shareowners, and minority or non controlling shareowners – within an organization. At its core, corporate governance is the arrangement of checks, balances, and incentives a company needs, in order to minimize and manage the conflicting interests between insiders and external shareowners. Its purpose is to prevent one group from expropriating the cash flows and assets of one or more other groups.[25]

Summary and Conclusions

The internal control concept is crucial to business success. There are models and guidance and hundreds of specific measures that can be used to develop and maintain a good system of internal control. There are reporting standards that ask the board to report on internal control and ensure that this is linked to a suitable system for assessing risk and formulating a wider risk management strategy. Controls tend to form a major component of the risk management, and there are some controls that are standard requirements implicitly or explicitly. One bank was fined £750,000 for failing to install basic checks on customers to stop them laundering money through the British banking system. The FSA only reduced the fine to this amount when it was clear that the bank had taken steps to improve their controls. Some argue for a central force to pull together this idea of internal control and recommend the role of experts in control to address the fact that the architect is missing:

> No one in the organization has been officially assigned the responsibility of viewing internal control as an entity-wide phenomenon. No one is in charge – there is no designated expert with vision, design theory, and astute understanding of practical, effective policies and their potential behavioral impact on personnel. Although internal auditors play a key role in the internal control process, they are not formally recognised as the designers of the system. Instead, auditors either monitor existing systems and provide suggestions about weaknesses that should be corrected or provide consultation to members of management who wish to discuss ways of improving the system. Internal control appears to be fragmented, and the function that should be at the beginning of the process is a missing link. Perhaps it's time for a new function – one that is headed by an expert in control processes who designs the entity's overall system and coordinates all aspects of implementation. Certainly, leadership in this area seems to be required in today's organizations. Architects are sorely needed.[26]

COSO have worked hard to establish a workable control framework and pose a strong argument that:

> Internal control can help an entity achieve its performance and profitability targets, and prevent loss of resources. It can help ensure reliable financial reporting. And it can help ensure that the enterprise complies with laws and regulations, avoiding damage to its reputation and other consequences. In sum, it can help an entity get to where it wants to go, and avoid pitfalls and surprises along the way.

If there is a sound system of corporate governance in place and if this underpins a robust control environment then an organisation may develop a control policy, perhaps as part of the risk policy. Where these considerations have been addressed, control awareness training may be carried out to turn ideas into practice. Where none of the control infrastructure that has been mentioned is in place, board awareness seminars on internal control may be used to start the ball rolling. The internal auditor needs to be able to assess the organisation in terms of these types of issues before any useful internal audit work can begin. The consulting role of internal audit argues that the auditor may help set up the necessary infrastructure (control framework) while the assurance role suggests that internal audit can go on to make sure the framework is owned by managers and that it makes sense and works well. It is difficult to talk about risk management without talking about internal control, as they are both necessary aspects of ensuring the business succeeds. For the private sector, control is really about survival. For public sector services, a wonderful summary of the importance of internal control is found in the guidance issued by the State of New York, Office of the State Comptroller who explained that:

> Citizens demand and deserve cost effective government programs. They also expect to receive value for their tax dollars. Over the years, my auditors have been able to trace almost every major shortcoming they have identified in government programs, from lack of program accomplishment or results to wasteful or fraudulent activity, to a breakdown on some component of the systems of internal control. If government organizations are to be effective, we must establish and maintain a system of internal control to protect government resources against fraud, waste, mismanagement or misappropriation. Employees often underestimate the importance of internal controls, or think internal controls amount to merely separating duties. However, internal controls encompass a comprehensive system that is critical to helping an organization achieve its goals and mission. A good system of internal control can do this because it helps you manage risk and run your agency's programs and administrative activities effectively and efficiently.[27]

Chapter 4: Assignment Questions

Having worked through the chapter the following questions may be attempted (see Appendix A). Note that the question number relates to the section of the chapter that contains the relevant material.

1. Explain the importance of internal controls to a business and describe management's responsibilities regarding these controls.
2. Describe the COSO control framework and discuss each of the five components.
3. Describe the CoCo control framework and discuss each of the components.
4. Discuss some of the issues addressed by other control standards such as BASEL and COBIT.
5. Explain the link between risk management and internal control.

6. Describe the different types and categories of controls that exist in most large organisations and explain what could go wrong, even where controls are meant to be in place.
7. Discuss the importance of good operational procedures and how such procedures might be established within an organisation.
8. Describe some of the issues addressed in the control model used in this chapter and explain the way each component of the model contributes to promoting good controls.
9. Discuss the view that controls can only provide reasonable and not absolute assurances that objectives will be achieved.
10. Prepare a presentation to the internal audit management team on developing and implementing control awareness seminars for key staff across the organisation.

Chapter 4: Multi-Choice Questions

4.1 Which is the most appropriate statement?

a. Where there are risks to the achievement of objectives, this means failure is a strong possibility, and controls have to be put in place to address these risks. If not, success becomes likely. At the same time, controls cost money and they have to be worthwhile.
b. Where there are risks to the achievement of objectives, this means failure is a strong possibility, and controls have to be put in place to address these risks. If not, failure becomes likely. At the same time, controls save money and they have to be worthwhile.
c. Where there are risks to the achievement of objectives, this means failure is a strong possibility, and controls have to be put in place to address these risks. If not, failure becomes likely. At the same time, controls cost money and they have to be worthwhile.
d. Where there are risks to the achievement of objectives, this means failure is a strong possibility, and controls have to be put in place to address these risks. If not, failure becomes likely. At the same time, controls save money and they are worthwhile.

4.2 Insert the missing phrase:

The Turnbull Report suggests that: A company's system of internal control has a key role in the management of risks that are significant to the fulfilment of its business objectives. A sound system of internal control contributes to safeguarding the ..... and the company s assets.

a. shareholders' investment
b. stakeholders' investment
c. shareholders' risks
d. stakeholders' risks

4.3 Insert the missing phrase:

The ..... should also set the tone of the company and cover ethical values, management's philosophy and the competence of employees.

a. control environment
b. ethical environment
c. risk framework
d. value system

4.4 Which is the most appropriate statement?

a. Effective controls are measures that work and ensure that operations are successful and resources protected.
b. Effective controls are measures that work and give a reasonable probability of ensuring that operations are successful.

c. Effective controls are measures that work and give a reasonable probability of ensuring that operations are successful and resources protected.
d. Effective controls are measures that work and give a reasonable probability of ensuring that resources are protected.

4.5 Which is the odd one out?
Turnbull provides some background as to what makes up a sound system of internal control: an internal control system encompasses the policies, processes, tasks, behaviours and other aspects of a company that, taken together:
a. facilitate its effective and efficient operation by enabling it to respond appropriately to significant business, operational, financial, compliance and other risks to achieving the company's objectives. This includes the safeguarding of assets from inappropriate use or from loss and fraud, and ensuring that liabilities are identified and managed;
b. help ensure the quality of internal and external reporting. This requires the maintenance of proper records and processes that generate a flow of timely, relevant and reliable information from within and outside the organisation;
c. help define how employees should be disciplined;
d. help ensure compliance with applicable laws and regulations, and also with internal policies with respect to the conduct of business.

4.6 Insert the missing phrase:
The trend towards ..... where each business audit is pretty well autonomous depends on a series of boundaries set at local levels throughout the organisation.
a. centralized organisations
b. structured organisations
c. fragmented organisations
d. devolved organisations

4.7 Insert the missing phrase:
It is only be considering the ..... that the internal auditor is able to make board level declarations concerning internal control.
a. adopted controls
b. adopted control model
c. approved controls
d. individual internal controls

4.8 Which is the odd one out?
Each component of the COSO model is listed:
a. Control Environment
b. Risk Assessment
c. Risk Management
d. Control Activities
e. Information and Communication
f. Monitoring

4.9 Which is the most appropriate statement?
The Control Environment has been described by COSO as
a. The control environment sets the tone of an organisation, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.
b. The control environment sets the tone of an organisation, influencing the control consciousness of its people. It is one aspect of internal control, providing discipline and structure.

c. The control environment sets the tone of an organisation, influencing the control compliance by its people. It is one aspect of internal control, providing discipline and structure.
d. The control environment sets the tone of an organisation, influencing the control consciousness of its senior management. It is the foundation for all other components of internal control, providing discipline and structure.

4.10 Which is the most appropriate statement?
Risk assessment has been described by COSO as
a. Every entity faces a variety of risks from internal sources that must be assessed. A precondition to risk assessment is establishment of objectives, linked at different levels and internally consistent.
b. Every entity faces a variety of risks from external sources that must be assessed. A precondition to risk assessment is establishment of objectives, linked at different levels and internally consistent.
c. Every entity faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is establishment of objectives, linked at different levels and internally and externally consistent.
d. Every entity faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is establishment of objectives, linked at different levels and internally consistent.

4.11 Which is the most appropriate statement?
Control Activities have been described by COSO as
a. Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the entity's objectives.
b. Control activities are the policies and procedures that help ensure management directives are understood. They help ensure that necessary actions are taken to address risks to achievement of the entity's objectives.
c. Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the manager's objectives.
d. Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to eliminate risks to achievement of the entity's objectives.

4.12 Which is the most appropriate statement?
Information and Communications has been described by COSO as
a. Pertinent information must be identified, captured and communicated in a form and time frame that enable people to carry out their responsibilities. Information systems produce reports, containing operational information, that make it possible to run and control the business.
b. Pertinent information must be identified, captured and communicated in a form and timeframe that enable people to carry out their responsibilities. Information systems produce reports, containing financial and compliance-related information, that make it possible to run and control the business.
c. Pertinent information must be captured and communicated in a form and timeframe that enable people to carry out their responsibilities. Information systems produce reports, containing operational, financial and compliance-related information, that make it possible to run and control the business.

d. Pertinent information must be identified, captured and communicated in a form and timeframe that enable people to carry out their responsibilities. Information systems produce reports, containing operational, financial and compliance-related information, that make it possible to run and control the business.

4.13 Which is the most appropriate statement?

Monitoring has been described by COSO as

a. Internal control systems may need to be monitored – a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two.
b. Internal control systems need to be monitored – a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two.
c. Internal control systems need to be monitored – a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities or separate evaluations.
d. Internal control systems need to be monitored – a compliance process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two.

4.14 Which is the odd one out?

COSO simply asks several key questions:

a. Do we have the right foundations to control our business?
b. Do we understand all those risks that stop us from being in control of the business?
c. Have we implemented suitable control activities to address the risks to our business?
d. Are we able to monitor the way the business is being controlled?
e. Are financial controls properly differentiated from operational controls?
f. Is the control message driven down through the organisation and associated problems and ideas communicated upwards and across the business?

4.15 Please list the main components of CoCo

a.
b.
c.
d.
e.

4.16 Which is the most appropriate statement?

a. The equation is quite simple. Controls are needed if they guard against an unacceptable risk to the business or if they are part of a legal or regulatory compliance regime.
b. The equation is quite complex. Controls are needed if they guard against an unacceptable risk to the business or if they are part of a management directive.
c. The equation is quite simple. Controls are needed if they guard against an unacceptable risk to the business or if they are part of a management directive.
d. The equation is quite simple. Controls are needed if they guard against an unacceptable risk to the finances or if they are part of a legal or regulatory compliance regime.

4.17 Which is the odd one out?

Control mechanisms are all those arrangements and procedures in place to ensure the business objectives may be met and they should exhibit certain defined attributes:

a. They should be clearly defined and understood by all users.
b. Mechanisms should be established to monitor the extent to which control is being applied in practice.

c. Controls should be reviewed annually.
d. Their use should be agreed by management and the staff who operate them.

4.18 Insert the appropriate code (Dir, P, Det or C after each example below.

Another way to classify controls is to break them down into: Directive **(Dir)**, Preventive **(P)**, Detective **(Det)** and Corrective **(C)**:

a. Fire alarms
b. Staff awareness training where the importance of guarding against fire
c. Fire appliances and fire extinguishes
d. Banning unauthorized electrical appliances

4.19 Which two are the odd ones out?

In terms of assessing the suitability of systems of internal control, there are some danger signs that should be looked for that might lower the efficiency of the control environment as follows:

a. Ability of senior management to override accepted control
b. Absence of documentation for all day-to-day decisions that are made
c. Lack of staff and vacant posts
d. Poor control culture
e. Staff collusion
f. Use of contingency arrangements for unusual situations
g. Reliance on a single performance indicator
h. Reliance on memory
i. Retrospective transaction recording
j. Uncontrolled delegation of tasks.

4.20 Insert the missing word:

It has been said about the importance of understanding soft controls:

As managements move into ..... modes, they need help with the transition. Most of all, they need us to be an independent, objective observer who will give them the kind of realistic, honest, substantial feedback that most people in the organisation won't provide.

a. fire fighting
b. performance
c. empowerment
d. supervisory

4.21 Insert the missing phrase:

There is a view that the auditor should know more about the system under review than management and as such may tell them how best to perform their managerial duties. This is false since it is managers who must understand their areas of responsibility and audit's role is not to ..... them.

a. challenge
b. second-guess
c. criticize
d. upset

4.22 Which is the odd one out?

By going through the nine-point stage model, there is a better change to get procedures both correct, understood and accepted in the operation in question. Taking each stage of the model in turn:

1. **Development**: This involves reviewing the underlying processes, simplifying them and working with users – then drafting an agreed document that reflects the required activities.
2. **Induction**: It is important to introduce the procedure to new starters and show existing staff a new or improved procedure.
3. **The training manual**: This may be broken down into two levels. Where staff are assessed as able to apply procedures, an outline manual ('a') can be provided. Where this is not the case, a more comprehensive package ('a&b') with exercises can be given to them to work through.
4. **Outline**: After the training or induction period, it is possible to turn to a short-cut outline document with key tasks and processes summarized for use thereafter.
5. **Training**: The skills of staff affect the degree to which procedures are successful. The training on procedures is mainly about knowledge and to supplement this, we should also seek to develop the underlying skills and the appropriate attitudes as a parallel training initiative.
6. **Documentation**: After the training has been completed, staff should be given a detailed document setting out the procedure and a list of key tasks that need to be performed each day.
7. **Appraisal**: This links the way staff are using procedures in their performance appraisal framework. In this way, it is seen to have some meaning to the work people do and their individual development programmes.
8. **Discipline**: This is a fall-back position, where if all else fails, staff may need to be disciplined for breach of procedure.
9. **The review process**: This should be straightforward in that it entails keeping the procedure relevant, vibrant and up-to-date.
10. **Compliance**: This stage deals with compliance and it is the line manager's responsibility to ensure staff comply with procedure. This is best done by getting staff to understand how they can monitor themselves, and supporting them in this task.

4.23 Which is wrong?

Measures are needed to give the organisation its best chance of achieving success. To sum up, it may be suggested that

a. controls tend to cost money and slow an organisation down.
b. controls are needed to help manage risks to an organisation's business.
c. controls can guarantee success.
d. control is effected through people and dependent on the way they behave and relate to each other.
e. even the best-managed organisation can fail.

4.24 Insert the missing phrase:

This is important so that control frameworks don't just contain activities, but also allow for some experimentation and innovation, that ..... but still sit within the constitution. An enterprise may give someone a budget and tell them to go away for a month and come back with new ideas, in any way they deem appropriate.

a. break the rules
b. break the law
c. break the bank
d. break the spirit

4.25 Which is the odd one out?

The success of control awareness training depends in part on several main drivers:

a. a corporate policy on risk and internal control.
b. a zero tolerance policy in terms of errors and sick leave.
c. the board's involvement.
d. staff competencies that include a good understanding of internal control concepts, design and review.
e. a resource (trainer) that is able to lead the training event.
f. a commitment to sound controls that means time is found for training programmes.

4.26 Insert the missing words:

If there is a sound system of corporate governance in place and if this underpins a robust control environment then an organisation may develop a control policy, perhaps as part of the risk policy. Where these considerations have been addressed, control awareness training may be carried out to turn ideas into practice. Where none of the control infrastructure that has been mentioned is in place, board awareness seminars on internal control may be used to start the ball rolling. The internal auditor needs to be able to ..... before any useful internal audit work can begin.

a. assess the audit service in terms of its reputation
b. assess the regulations in terms of these types of issues
c. assess the level of non compliance with procedures
d. assess the organisation in terms of these types of issues

References

1. Moeller Robert and Witt Herbert (1999) *Brink's Modern Internal Auditing*, 5th edition, New York: John Wiley and Sons Inc.
2. 'Book sale lost £32m'. *Accountancy Age*, 19 Feb. 1998, p. 3.
3. Flesher Dale (1996) *Internal Auditing: A One-Semester Course*, Florida: The Institute of Internal Auditors, p. 127.
4. The Combined Code on Corporate Governance, Jun. 2008, Financial Reporting Council.
5. Moeller Robert and Witt Herbert (1999) *Brink's Modern Internal Auditing*, 5th edition, Para. 2.3, New York: John Wiley and Sons Inc.
6. *Daily Mail*, 10 Nov. 2001, p. 35, 'Jail for woman banker who stole £1.75 million'.
7. Smith Philip 0'Reining in the rogue traders'. *Accountancy Age*, 12 Oct. 2000, p. 6.
8. Arkin Anat 'Return to centre'. *People Management*, 6 May 1999.
9. Gibbs Jeff and Gibson Susan 'Organizational effectiveness.' *Internal Auditor*, Feb. 1998.
10. Anderson Urton and Chapman Christy IIA 2002 in The IIA Handbook Series, *Implementing The Professional Practices Framework*, p. 91.
11. Simmons Mark R. 'COSO The standards and the framework.' *Internal Auditor*, April 1997.
12. Jackson Peter Director of Criteria of Control at CICA. 'COCO In the crucible'. *Camagazine*, June/July 1998, p. 41.
13. Internal Control: Providing a Foundation for Accountability in Government, an Introduction to Internal Control for Managers in Government Organizations, the International Organization of Supreme Audit Institutions 2001, the Internal Control Standards Committee.
14. Framework for Internal Control Systems in Banking Organisations, Basel Committee on Banking Supervision, Basel, Sept. 1998 (www.bis.org).
15. Interview with Roth Jim 'A hard look at soft controls'. *Internal Auditor*, Feb. 1998, pp. 31 – 33.
16. Spencer Pickett K. H. S. and Pickett Jennifer M. (2001) *Internal Control: A Manager's Journey*, New York: John Wiley and Sons Inc.
17. Hope Tony and Hope Jeremy 'Chain reaction'. *People Management*, 25 Sept. 1997, p. 26.
18. McNamee David and Selim Georges *Internal Auditor*, June 1999, p. 36.
19. Nasa Policy Directive – 1 June 2000, Internal Management Controls and Audit Liaison and Follow-Up (www.nasa.gov).

20. Sawyer Lawrence B. and Dittenhofer Mortimer A. Assisted by Scheiner James H. (1996) *Sawyer's Internal Auditing*, 4th edition, Florida: The Institute of Internal Auditors.
21. Pickett K. H. S. and Pickett Jennifer M. (2001) *Internal Control: A Manager's Journey*, New York: John Wiley and Sons Inc., p. 225.
22. Financial Reporting Council, July 2009, Review of the Effectiveness of the Combined Code, Progress Report and Second Consultation.
23. Quirk Barry 'Blame, shame and leadership'. *Public Finance*, 3–9 Dec. 1999, p. 16.
24. Internal Auditing & Business Risk, IIA Magazine, Oct. 2008. Internal Auditing PAGE 35, Eddie Best.
25. (2009) *The Corporate Governance of Listed Companies: A Manual for Investors*, 2nd edition: CFA Institute Centre for Financial Market Integrity, p. 3.
26. Oliverio Mary Ellen 'In my opinion, the architect is missing'. *Internal Auditor*, February 2002, p. 76.
27. State of New York, Office of the State Comptroller, US, Feb. 1999 (www.osc.state.ny.us).

Chapter 5

THE INTERNAL AUDIT ROLE

Introduction

This chapter covers the role of internal auditing and describes what it takes to become a good auditor.

Note that all references to IIA definitions, code of ethics, IIA attribute and performance standards, practice advisories and practice guides relate to the IPPF prepared by the IIA in 2009. The areas covered are

5.1 Why Auditing?
5.2 Defining Internal Audit
5.3 The Audit Charter
5.4 Audit Services
5.5 Independence
5.6 Audit Ethics
5.7 Police Officer versus Consultant
5.8 Managing Expectations through Web Design
5.9 Audit Competencies
5.10 Training and Development
5.11 New Developments
Summary and Conclusions
Assignments and Multi-choice Questions

The challenges for the internal audit profession are found in the early chapters of the book, that is corporate governance, risk management and control. These developments set the context for the audit role. Now we need to explore how such challenges may be met.

5.1 Why Auditing?

Before we delve into the standard features of the internal audit role, we issue a challenge to the reader. Andy Wynne, of the ACCA, has described the internal audit role in terms of the scope to help management cope with complicated systems that change and evolve over time. In an interesting piece written specially for the new Handbook, these issues are explored by Andy in his paper entitled 'Dialectics and Internal Audit':

> 'Nothing endures but change' – Heraclitus 540–480 BC
>
> Classical logic is based on a philosophy that assumes a fundamentally unchanging universe. The seasons may change but the cycle will repeat itself. Most observers now recognise that the only constant factor in our lives is change. However, many people seem to believe that this is an aberration and there is an unspoken assumption that sooner or later we will return

to the good old days of stability. In a constantly changing world this is not an accurate model of our universe and on the contrary classical logic is not acceptable, especially for those of us who need to have a clear understanding of our organisation and its expectations for the future. We need an alternative philosophy or logic that more clearly matches and reflects our organisations and the society in which we live. I believe that dialectics provides that logic. It is based on three premises, change, totality and contradiction. Dialectics accepts that change is fundamental to all systems, processes, organisations and society. For internal auditors accepting that all systems are subject to constant change is an important step to understanding control systems and the risks that our organisations face now and those they may face in the future. We have to ensure that the systems we review are robust enough to survive this constant change. Change occurs both internally and externally. Externally our organisations face an ever-changing and largely unpredictable environment. Its control systems and risk management processes need to take account of this changing environment. Contingency planning needs to be a key aspect of all systems. Will the systems still operate effectively if key staff are absent due to sickness, strikes, transport problems etc.? Will the systems and information still be available in circumstances of extended power failure or communication problems, loss of telephone or mail facilities for example? How will the organisation respond when its funding is significantly reduced or increased? Internally organisations are also subject to constant change. Systems may operate well with the current staff, but how will new staff be trained to take over or fill in? When reorganisation takes place or staff take on further responsibilities will the system still be as effective as it is now? Major changes may be easily identified and steps taken to reduce their input, but minor changes are also important. Dialectics recognises this and has identified that the cumulative impact of a series of small changes can have a major impact on organisations and moreover they may not be recognised until it is too late. An analogy may be made with the growth of water weed in a pond. If a small amount of weed is growing rapidly this may not be noticed even if it doubles in size each day. Two days before it completely covers the pond it will only cover a quarter of the pond and may not be recognised as a major problem. If it is only recognised the next day when it covers half the pond it will be too late. The next day the whole pond will be covered. The cumulative effect of small changes is important for internal auditors. This is the reason that, even in relatively well controlled work places, key systems should be reviewed regularly. The corrosive effect of change will degrade even the most carefully controlled systems given enough time. We need to ensure that corrective action is taken before the effects of these changes become significant. The second aspect of dialectics is a recognition that all processes, systems and organisations are part of a totality. For ease and simplicity we break down the interrelated processes within our organisations into a number of systems and usually assume these are discrete and review them one at a time. But we cannot divorce the particular system we are reviewing from related systems, the whole organisation and indeed the whole of society. For us to fully understand the system we are currently reviewing we have to consider the big picture and how changes and inter-relationships with other parts of the organisation may affect the controls within the system and the risks they are designed to reduce. For us to be successful internal auditors we have to try and understand this totality and see each system that we review as part of the whole control system, organisation and ultimately society. The concept of totality or inclusivity should also be applied to internal audit staff. They are subject to the same pressures and temptations as other staff and as a result should be controlled to the same degree. Internal audit is not a function that operates independently or outside of an organisation with a separate breed of super staff. We are part of the systems or organisations we review and should be seen and treated in this light. The final aspect of dialectics is contradiction. This recognises that all staff within an organisation do not have the same objectives and that the objectives that staff have may be contradictory. This may be seen clearly in the contradictory objectives that senior managers have and those held by many of the

people working within their organisation. Senior managers want the people working for them to work harder, faster and usually for the same or preferably less money. The people who work for them usually want the opposite, an easy life and more money! The recognition of contradictory objectives and viewpoints is important for internal auditors. When we are recommending particular changes we have to recognise that these will not be perceived as neutral. They may be agreed by managers, but not all staff; one section may welcome the suggestion; another may see it as a threat. To be effective we should recognise these contradictory views and consider how they should be addressed by the organisation. Society is an internally contradictory totality in a constant process of change. The whole cannot be reduced to the parts, as the parts and the whole mutually condition or mediate each other. These and other insights that dialectics provide us are important and should enable internal auditors to better understand their organisation and so be more effective. We have to look at the totality when we are reviewing any system. There are two dimensions to this that are particularly important for internal auditors. One is that controls do not exist for themselves, but are needed to ensure that the objectives of the specific system are achieved more efficiently. Secondly the individual systems also do not exist for themselves. Internal auditors need to consider ways that, for example, the payroll system furthers the objectives of the whole organisation and, at a higher level still, we should consider the extent that the success of the whole organisation is dependent on the way that its objectives agree with the objectives of the society we live in.

5.2 Defining Internal Audit

The starting place for internal audit theory is the definition of internal audit. A standard definition is made up of important issues that form the basic framework of internal audit principles. The divergence of interpretation of the audit role is explored in terms of the way we may in practice move away from the standard definition. Internal auditing is performed in a variety of ways, each with its own approach and style. Accordingly, it is important that a formal definition is devised and agreed since it will have a vital impact on the perceived role of the audit function. Management often asks auditors exactly what they are responsible for, and a variety of responses may be received. Some auditors feel that they should police the organization while others are convinced they must check the accuracy of accounting records. Still others feel obliged to search out poor value for money or new and improved ways of using resources. Much depends on the audit charter and management expectations. One must have a model developed by the profession which represents the true scope of internal auditing. In this model, management is clearly responsible for controlling risks to ensure objectives are met, while the scope of audit work is based on reviewing risk management and controls.

The Institute of Internal Auditor's (IIA) Definition

> Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.

Although brief, it contains the basic principles on which internal audit is based. Meanwhile IIA Performance Standard 2100 deals with the nature of internal audit's work and says that:

> The internal audit activity must evaluate and contribute to the improvement of governance, risk management, and control processes using a systematic and disciplined approach.

We can analyse the IIA's formal definition in detail by examining each of the material concepts:

'Internal auditing' The service is provided within the organization and is distinct from the external audit role (but see 'activity' below). Years ago the IIA considered changing the name of internal auditing to reflect the modern and increasingly professional approach. No alternative was forthcoming and the idea was dropped.

'Independent' The concept of independence is fundamental. Internal auditing cannot survive if it is not objective. All definitions of internal audit feature an element of independence, although its extent, and how it is achieved, is a topic in its own right. The audit function must have sufficient status and be able to stand back from the operation under review for it to be of use. If this is not achieved, then this forms a fundamental flaw in the audit service and some internal audit functions may not be able to subscribe to the standards.

'Assurance and consulting' This part of the definition refers to the fundamental shift in the role of internal audit. The shift makes clear that the past tinkering with the advice and consulting aspect of auditing is now a full-blown additional consultancy arm of the function. Internal audit may provide advice and assistance to management in a way that best suits each manager's needs. Even consulting work should take on board the impact of risks and IIA Performance Standard 2120.C1 says that:

> During consulting engagements, internal auditors must address risk consistent with the engagement's objectives and be alert to the existence of other significant risks.

Meanwhile, the primary role of internal audit is to provide independent assurances that the organization is, or is not, managing risk well. Internal audit can provide assurance on the extent to which controls are able to address risks but cannot give any absolute guarantees.

'Activity' The fact that the internal audit function is an activity is important. This means it is a defined service, although not necessarily located within the organization (e.g. it may be outsourced) as has been the case with past definitions.

'Designed to add value' As a service, auditing has to form a client base and understand the needs of the organization. Here the service role should lead to a defined benefit to the organization rather than internal audit working for its own mysterious goals. Adding value should be uppermost in the minds of CAEs and this feature should drive the entire audit process.

'And improve an organization's operations' This brings into play the notion of continuous improvement. The auditors are really there to make things better and not inspect and catch people out. In one sense, if the CAE cannot demonstrate how the auditors improve the business, there is less reason to resource the service.

'It helps an organization accomplish its objectives' The task of internal audit is set firmly around the organization's corporate objectives. Making an organization successful is the key driver for corporate governance (a badly governed organization will not be successful), for risk management (where risks to achieving objectives is the main focus) and internal controls (that seek to ensure objectives are realized). Moreover, it is the search for long-term corporate success that must steer the internal audit shop, or there is little point setting up the team.

'Systematic, disciplined approach' Internal audit is now a full-blown profession. This means it has a clear set of professional standards and is able to work to best practice guidelines in delivering a quality service. One measure of this professionalism is that the organization can expect its auditors to apply a systematic and disciplined approach to its work. Be it consulting or assurance work, IIA Performance Standard 2040 requires that:

> The chief audit executive must establish policies and procedures to guide the internal audit activity.

'Evaluate and improve' We have mentioned the need to focus on making improvements in the organization and part of this search for improvement entails making evaluations. Internal audit sets what is found during an audit against what should be present to ensure good control. This necessarily entails the use of evaluation techniques that are applied in a professional and impartial manner to give reliable results. Many review teams leave out the evaluation aspect of review work and simply ask a few questions or check a few records and their results are not robust. Internal audit, on the other hand, has built into its definition the formal use of evaluation procedures to support steps to improve operations.

'Effectiveness' Effectiveness is a bottom-line concept based on the notion that management is able to set objectives and control resources in such a way as to ensure that these goals are in fact achieved. The link between controls and objectives becomes clear, and audit must be able to understand the fundamental needs of management as it works to its goals. The complexities behind the concept of effectiveness are great, and by building this into the audit definition, the audit scope becomes potentially very wide.

'Risk management, control and governance processes' These three related concepts have been covered in early chapters of the book and set the parameters for the internal audit role. Organizations that have not developed vigorous systems for these matters will fail in the long run and fall foul of regulators in the short term. The internal auditors are the only professionals who have these dimensions of corporate life as a living and breathing component of their role. They should therefore be the first port of call for anyone who needs to get to grips with corporate governance and IIA Performance Standard **2120 states:**

> The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes. Determining whether risk management processes are effective is a judgment resulting from the internal auditor's assessment that:
>
> - Organizational objectives support and align with the organization's mission;
> - Significant risks are identified and assessed;
> - Appropriate risk responses are selected that align risks with the organization's risk appetite; and
> - Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.

Risk management processes are monitored through ongoing management activities, separate evaluations, or both.

The assurance role of internal auditing needs to be understood. Assurance implies a form of guarantee that what appears to be the case is in fact the case, based on a reliable source of confirmation that all is well. The more impartial and professional the source of these assurances

the more reliable they become. The importance of this assurance process is well described by Sarah Perrin:

> The assurance service provided by and sought by internal audit teams generally evolve over time. The internal audit function at Kalon Group has been up and running for just two years. Through acquisition the company found itself moving within a year from a British company to one with a presence in 27 countries and head office needed reassurance that reported figures from these locations were reliable. 'My remit is to give comfort to the audit committee that acceptable controls, processes and practices are in place throughout the organization,' says David O'Regan, head of internal audit. 'It focuses heavily on the accounting and financial side, to provide comfort that accounting and financial processes are being adhered to'.[1]

Is There a Right Model?

Several well-known authorities have used definitions outside of the IIA standards:

CIPFA definition

> Internal audit is an independent and objective appraisal service within an organization: Internal audit is an assurance function that primarily provides an independent and objective opinion to the organization on the degree to which the internal control environment supports the achievement of the organization's objectives. The internal control environment comprises the policies, procedures and operations established to ensure the achievement of objectives, the appropriate assessment of risk, the reliability of internal and external reporting and accountability processes, compliance with applicable laws and regulations, and compliance with the behavioural and ethical standards set for the organization. In addition, internal audit's findings and recommendations are beneficial to line management in the audited areas. Internal audit can also provide an independent and objective consultancy service specifically to help line management improve the organization's internal control environment. The service applies the professional skills of internal audit through a systematic and disciplined evaluation of the policies, procedures and operations that management put in place to ensure the achievement of the organization's objectives, and through recommendations for improvement. Such consultancy work can contribute to the opinion which internal audit provides on the internal control environment.

The 2006 Code of Practice for Internal Audit in Local Government in the United Kingdom has the following elements:

Introduction	
	THOSE CHARGED WITH GOVERNANCE
	DEFINITION OF INTERNAL AUDIT
	COMPLIANCE WITH THE CODE
Standard 1	**Scope of Internal Audit**
	1.1 TERMS OF REFERENCE
	1.2 SCOPE OF WORK
	1.3 OTHER WORK
	1.4 FRAUD AND CORRUPTION
Standard 2	**Independence**
	2.1 THE PRINCIPLES OF INDEPENDENCE
	2.2 ORGANIZATIONAL INDEPENDENCE

2.3 STATUS OF THE HEAD OF INTERNAL AUDIT
2.4 INDEPENDENCE OF INDIVIDUAL INTERNAL AUDITORS
2.5 INDEPENDENCE OF INTERNAL AUDIT CONTRACTORS
2.6 DECLARATION OF INTEREST

Standard 3 **Ethics for Internal Auditors**
3.1 PURPOSE
3.2 INTEGRITY
3.3 OBJECTIVITY
3.4 COMPETENCE
3.5 CONFIDENTIALITY

Standard 4 **Audit Committees**
4.1 PURPOSE OF THE AUDIT COMMITTEE
4.2 INTERNAL AUDIT'S RELATIONSHIP WITH THE AUDIT COMMITTEE

Standard 5 **Relationships**
5.1 PRINCIPLES OF GOOD RELATIONSHIPS
5.2 RELATIONSHIPS WITH MANAGEMENT
5.3 RELATIONSHIPS WITH OTHER INTERNAL AUDITORS
5.4 RELATIONSHIPS WITH EXTERNAL AUDITORS
5.5 RELATIONSHIPS WITH OTHER REGULATORS AND INSPECTORS
5.6 RELATIONSHIPS WITH ELECTED MEMBERS

Standard 6 **Staffing, Training and Continuing Professional Development**
6.1 STAFFING INTERNAL AUDIT
6.2 TRAINING AND CONTINUING PROFESSIONAL DEVELOPMENT

Standard 7 **Audit Strategy and Planning**
7.1 AUDIT STRATEGY
7.2 AUDIT PLANNING

Standard 8 **Undertaking Audit Work**
8.1 PLANNING
8.2 APPROACH
8.3 RECORDING AUDIT ASSIGNMENTS

Standard 9 **Due Professional Care**
9.1 PRINCIPLES OF DUE PROFESSIONAL CARE
9.2 RESPONSIBILITIES OF THE INDIVIDUAL AUDITOR
9.3 RESPONSIBILITIES OF THE HEAD OF INTERNAL AUDIT

Standard 10 **Reporting**
10.1 PRINCIPLES OF REPORTING
10.2 REPORTING ON AUDIT WORK
10.3 FOLLOW-UP AUDITS AND REPORTING
10.4 ANNUAL REPORTING AND PRESENTATION OF AUDIT OPINION

Standard 11 **Quality**
11.1 PRINCIPLES OF PERFORMANCE, QUALITY AND EFFECTIVENESS
11.2 QUALITY ASSURANCE OF AUDIT WORK
11.3 PERFORMANCE AND EFFECTIVENESS OF THE INTERNAL AUDIT SERVICE

Government Internal Audit Manual

Internal audit is an independent and objective appraisal service within an organization:

- Internal audit primarily provides an independent and objective opinion to the Accounting Officer on risk management, control and governance, by measuring and evaluating their effectiveness in achieving the organization's agreed objectives. In addition, internal audit's findings and recommendations are beneficial to line management in the audited areas. Risk management,

control and governance comprise the policies, procedures and operations established to ensure the achievement of objectives, the appropriate assessment of risk, the reliability of internal and external reporting and accountability processes, compliance with applicable laws and regulations, and compliance with the behavioural and ethical standards set for the organization.

- Internal audit also provides an independent and objective consultancy service specifically to help line management improve the organization's risk management, control and governance. The service applies the professional skills of internal audit through a systematic and disciplined evaluation of the policies, procedures and operations that management put in place to ensure the achievement of the organization's objectives, and through recommendations for improvement. Such consultancy work contributes to the opinion which internal audit provides on risk management, control and governance.

There are many similarities in the various published definitions of internal auditing. Most revolve around the view of internal audit as an independent service to the organization reviewing systems of internal control. One useful model is quoted by Professor Gerald Vinten from unpublished course notes from a Masters degree programme, City University Business School, 1991. This emphasizes the need to direct audit resources at the future welfare of the organization as opposed to being preoccupied with past events in the form of recorded transactions and incidents that have already occurred:

> Internal auditing is the recurrent comprehensive investigation into apparently healthy organizations with the objective of achieving an insight into the state of the organization and also its environment with the objective of achieving better control over its future operations.

An audit department more concerned about future control issues than past events may have a dynamic impact on the organization although it requires a new approach to discharging the audit role. There is no one right model of internal audit and the final role adopted depends on the elements shown in Figure 5.1.

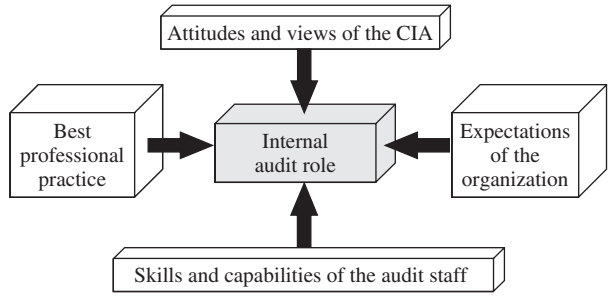


FIGURE 5.1 Factors impacting on the audit role.

The relative influence of each of these will define the final model of internal audit that is applied in an organization. The current trend is to move towards a consultancy-based approach that, as a result, is based on a very wide interpretation of the audit role. In this respect, special projects may be included in the range of work which in reality could mean almost anything that urgently needs doing. Best professional practice is based on the auditor discharging the requirements

of professional auditing standards. This represents an idealistic model but may be used as a suitable reference point. Organizational expectations become more significant in a market-led strategy where the client's needs are seen as paramount. Unfortunately, we cannot simply do what managers want us to do, as this would mean the audit function being indistinguishable from management consultants. The type of staff involved in discharging the audit role acts as a barrier to the resultant activities in that we can only perform work that staff are capable of performing. This becomes less material where qualified auditors are employed, in contrast to using all who happen to end up in the audit unit. The CAE has the final say in role definition as the person most responsible for delivering the defined services. The background and experience of this person will have great impact. This in turn is influenced by the job description that is drawn up as a basis for appointing the CAE. An organization establishing a new audit function is advised to use the services of an audit consultant to draw up terms of reference and recruit a suitable CAE.

The Four Main Elements

Let us return to the scope of internal auditing which is found in the IIA Performance Standard 2110.A1 which states that:

> The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the:
>
> - Reliability and integrity of financial and operational information.
> - Effectiveness and efficiency of operations.
> - Safeguarding of assets; and
> - Compliance with laws, regulations, and contracts.

Reliability and integrity of financial and operational information Internal auditors review the reliability and integrity of financial and operating information and the means used to identify, measure, classify and report such information.

Effectiveness and efficiency of operations Internal auditors should appraise the economy and efficiency with which resources are employed. They should also review operations or programmes to ascertain whether results are consistent with established objectives and goals and whether the operations are being carried out as planned.

Safeguarding of assets Internal auditors should review the means of safeguarding and, as appropriate, verifying the existence of such assets.

Compliance with laws, regulations and contracts Internal auditors should review the systems established to ensure compliance with those policies, plans, procedures, laws, regulations and important contracts which could have a significant impact on operations and reports, and should determine whether the organization is in compliance.

Internal audit reviews the extent to which management has established sound systems of internal control so that objectives are set and resources applied to these objectives in an efficient manner. This includes being protected from loss and abuse. Adequate information systems should be established to enable management to assess the extent to which objectives are being achieved via a series of suitable reports. Controls are required to combat risks to the achievement of

VFM and it is these areas that internal audit is concerned with. Compliance, information systems and safeguarding assets are all prerequisites to good VFM. There is a fundamental link between quality assurance and VFM as it is the quality systems that underpin the achievement of VFM. It may then be possible to restate the control objectives to read that controls are required for the achievement of organizational objectives in an efficient manner, ensuring that

- information systems and published reports are adequate,
- policies, procedures, laws and regulations are complied with,
- assets, including the corporate reputation, are protected.

Implications of the Wide Scope

The wide scope of internal audit has several implications:

1. Expertise Great expertise is required from auditors to enable them to provide advice on the wide range of key control objectives. Since we are charged with auditing anything and everything, we need some knowledge of almost all organizational activities. The ideal internal auditor may be the most experienced employee of the organization in terms of an overall knowledge of the different areas, second only to the chief executive. While this ideal is unrealistic it represents a major challenge for the auditor. Unfortunately, traditional internal audit departments who are locked into a never-ending annual cycle of checking the output from basic accounting systems will find it impossible to achieve the high standards that underpin this wide scope of audit work. A useful test is to ensure that audit reports interest the chief CEO as well as the DF. Resources directed at anything less than this may be of little use to the organization. Where the CEO assumes a risk and control orientation then the CAE must assume an educational role in promoting the right culture. This is easy if one considers that controls ensure organizational objectives are achieved. Once high standards have been established, this raises expectations which must be met. It can be achieved by implementing quality auditing systems in Figure 5.2.

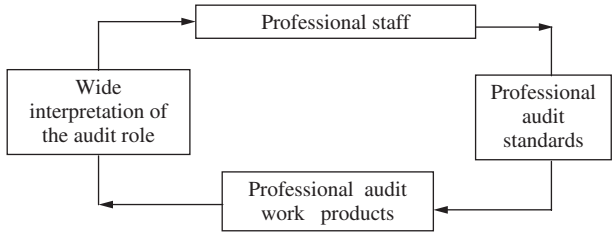


FIGURE 5.2 Ensuring quality audits.

2. Safeguarding assets It is necessary to establish who is responsible for investigating frauds since this is resource intensive. Where internal audit is wholly responsible for investigating fraud, error and irregularities, this may become a drain on audit resources. Adopting a wide scope of work and having the necessary skills to operate at this level will be of little use where most of the available time is spent responding to management referrals on matters of regularity. High-level fraud investigations do require an associated level of skills and there is potential for major impact on the organization. There is a defensive stance that may be assumed to preserve audit resources

that will be effective in the short term. This is to plan a comprehensive programme of compliance checks and verification routines to protect organizational assets. It is then possible to calculate the minimum resources to fund such a programme and it is in this way that the audit budget may be preserved. The main drawback is the need to deploy armies of junior resources to carry out the basic checks of compliance work, which militates against working to high professional standards. Balancing is required and this is the CAE's task. Management is, in the final analysis, responsible for safeguarding assets.

3. The compliance role Controls over compliance may include an inspection routine and audit's role in this should be clearly defined. Do we provide a probity-based service on behalf of management and visit all relevant locations or merely provide an advisory function to management on promoting compliance? It is useful for internal audit to be supported by a range of control teams located close to each operation as illustrated in Figure 5.3. This will work where the CAE sets up the following systems:

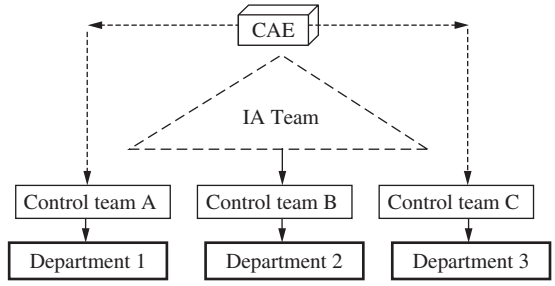


FIGURE 5.3 Compliance mechanisms.

- The control teams report to the appropriate department's director but the CAE has a functional responsibility for their work. This responsibility means that the CAE will be concerned with the standards and performance of the teams and want to see them excel. We would expect to see the CAE or a suitable representative present on any selection panel that chooses senior internal control staff.
- The control teams provide work programmes for each time period (e.g. each quarter) which will have to be approved by the CAE. This can work on a number of levels; it may simply involve receiving work plans for approval or being actively involved in their formulation. The important point is that these plans are wholly interfaced with the current internal audit plans.
- The control teams are required to furnish regular reports on progress against plan to the CAE (e.g. quarterly). The CAE may care to furnish the audit committee with this information. These reports constitute a major control over the teams in that they force them to formally account for their time as well as installing the discipline of weekly timesheet recording. Comparing planned against actuals is an accepted statistic that should highlight possible problems.
- The CAE will provide the teams with suitable procedures based around the audit manual that will set the direction and methodology of their work. This may become a slimmed down version of the audit manual dealing with basic probity checks that would form the basis of the control team's work. Furthermore, comprehensive audit programmes specially drafted for the control teams can be of great use, particularly where the team members are fairly new in their posts. This approach allows the CAE to review standards set via the audit manual.

- The CAE will carry out regular quality reviews of these teams and require that any operational deficiencies are corrected. Compliance with procedures will also be assessed. These reviews consider the extent to which the teams meet their stated objectives. It also allows the CAE to judge whether reliance can be placed on their work and so reduce any internal audit coverage.
- Where operational practices are adequate, the CAE will be able to issue internal audit warrants to the control teams that will allow them access to organizational records. Control teams will not ordinarily have access to most systems particularly those that are centralized or of a corporate nature. The power to issue or withhold audit warrants, which permit access across the organization, consolidates the CAE's functional responsibility over the control teams. It gives credence to the review process where material problems with their performance may result in a suspension or complete withdrawal of the warrant. As with all important powers this must be exercised with care.

4. Information systems The audit of MIS is crucial since this may involve reviewing MIS as part of operational audits, or these systems can be audited separately. MIS cannot be tackled without expertise. Auditing MIS may follow two main routes. We may review information systems as a concept in terms of looking at the way they are applied to enhancing the overall efficiency of operations. The assessment of MIS must be related to business objectives. The advantage is that one can concentrate expertise on the specific application that will almost certainly be computerized. Alternatively, it is possible to incorporate the assessment of MIS into all audits so that this becomes a fundamental feature of general audit work. This not only builds an appreciation of the importance of MIS by general auditors but also allows expertise to be acquired. It is easier to link MIS into business objectives when this information is viewed in conjunction with the wider elements of the audit. Moreover, information systems cannot be ignored and this is wholly within the scope of audit work.

5. Value for money The concept of economy, efficiency and effectiveness (or VFM) is another sensitive issue. Auditors can assist management's task in securing good arrangements for promoting VFM or alternatively undertake a continual search for waste and other poor VFM. These two different perspectives of the audit role will continue to arise in many different areas as it is based on the fundamental distinction between systems audits and investigations. A systems approach considers the managerial systems for addressing risks to VFM and judges whether this is working. Investigatory work, on the other hand, furnishes management with suggestions as to alternative operational methods. In terms of defining the scope of audit work, the former approach is purist auditing work that falls within our definition. The investigatory stance is more akin to a consultancy approach that, while in line with the scope of work, falls closer to a management role. VFM is relevant to audit work whatever the adopted approach. Andrew Chambers and Graham Rand have clarified the issues of what exactly is VFM:

> Value for money auditing takes account of the 3 Es. It frequently makes extensive use of performance indicators in the form of ratios and other statistics to give an indication of value for money – especially when trends are explored in these performance indicators over time, or variations in performance are identified and explained between different operating units. The term value for money is often applied to public sector spending in the UK, where there is an implied obligation placed on public bodies to ensure that they obtain and provide services on the most economic grounds. This process invariably involves elements of competition where cost comparisons are made between parties being invited to supply goods and services.[2]

6. Management needs A wide scope requires a good understanding of the operations being reviewed and it is necessary to include management's needs in the terms of reference by adopting a more participative style. Unlike the narrow approach that underpins traditional probity auditing, this depends on getting inside management objectives. It is then impossible to operate as outsiders and work primarily from documentation and records. This will hinder the ability to achieve high-level results. Close working arrangements with management are essential.

7. Specialists The four elements of the key control objectives may require specialists in each of the defined areas and the level of expectation may place great demands on the audit service. One might imagine that the audit function will eventually be broken down into defined fields with experts specializing in different ones. This point is explored below in the section on resourcing the wide scope of audit work.

Scope within Different Time Frames

Scope has been described as the range of audit work that may be performed within the overall terms of reference for the audit function. This concept is affected by the time frame applied. There are several relevant points:

1. Charter The major impact of the scope of audit work arises when the audit charter is being formulated, since this will set the whole direction of the audit function. A predetermined wide scope will necessarily require high profile, senior staff and an enhanced level of professionalism if it is to be achieved. These factors will have to be considered at conception stage, when the audit function is first set up.

2. Long-term plans The next level at which the question of scope is relevant appears at the long-term planning stage where an audit strategy is being devised. Here the scope of work will determine how audit work will be interfaced with the organization. Audit objectives and the way in which they fit into overall organizational needs will have to be defined in line with a comprehensive strategy for audit work. Since the scope of work partly sets out our responsibilities, there are obvious repercussions on the resultant strategy for discharging these responsibilities.

3. Medium-term plans Scope next appears on the agenda during the medium-term planning stage. It is here that the audit field is fully defined, risk analysis applied and a formal audit plan produced for consultation. The scope of audit work will apply here as it may be used to isolate the audit field and determine how these work areas will be tackled.

4. Assignment planning The final way in which scope is important is in terms of its impact on the assignment planning process. In practice, we will not be able to tackle all parts of a planned audit since in one sense every audit is open ended. It will be necessary to assess each business risk and then decide, through a process of preliminary review, which will be prioritized for the audit in question. The use of scope makes this task easier and sets a clear frame for the necessary assessment.

Resourcing the Agreed Scope

There are resource implications of adopting a wide scope of audit work that will have to be catered for by audit management. This is because the act of assuming the stance whereby

'everything of importance to controlling the organization will be audited' brings with it the need to meet these enhanced expectations. One might promise much, but it is the delivery of associated results that will be monitored, not mere statements of intent. The following illustration sets out the process of resourcing the wide scope of audit and how this might be managed in Figure 5.4.

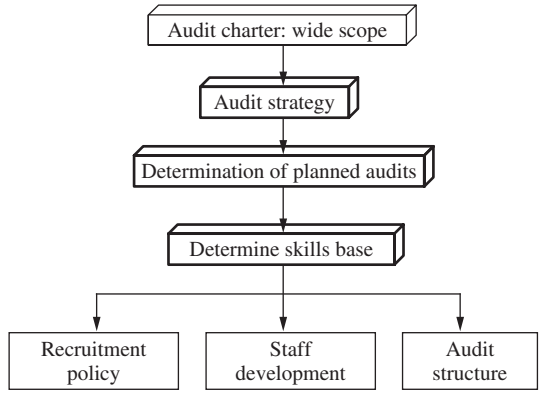


FIGURE 5.4 Resourcing the wide scope of audit work.

The idea is to ensure that the wide scope of audit work is taken into consideration when obtaining, developing and structuring audit staff. All relevant factors are accounted for when deciding how the agreed audit services will be delivered to management. While auditors are concerned about matters of compliance, information, fraud and VFM, one can use audit resources efficiently by advising management on steps they can take to manage risk and promote good controls in these areas. As long as resources have been applied to achieving a defined goal, an operation may be audited by considering Figure 5.5.



FIGURE 5.5 Audit components.

Internal audit may adopt an open-ended stance which suggests that anything may be subject to audit. This includes policies, major issues, structures, communications, attitudes and culture. The only caveat is the availability of skilled staff and reliable evidence to support such audits. The internal audit scope can be focused more clearly around key points of principles. Several noted writers have provided ways of achieving this clear direction:

Auditors must answer three questions: What should they audit? When should they audit it? For what purpose do they audit? First, the auditors should audit that part of the control system that produces the most benefit for the costs incurred. The costs include the audit staff's time and related expenses, such as travel. The benefits accrue from significant findings that improve control over key aspects of business operations. More importantly, benefits accrue from finding trouble spots and avoiding would-be losses. There also is a benefit from the 'threat value' of an audit. Even when there are no deficiencies found during an audit, the fact that members of the organization know that their activities are likely to be audited periodically often motivates improved performance and better internal control.[3]

5.3 The Audit Charter

The audit charter sets the agreed role and position of internal auditing in an organization and this is defined in the IIA's glossary of terms as:

> The internal audit charter is a formal document that defines the internal audit activity's purpose, authority, and responsibility. The internal audit charter establishes the internal audit activity's position within the organization; authorizes access to records, personnel, and physical properties relevant to the performance of engagements; and defines the scope of internal audit activities.

IIA Attribute Standard 1000 says that the:

> Purpose, authority, and responsibility of the internal audit activity must be formally defined in an internal audit charter, consistent with the Definition of Internal Auditing, the Code of Ethics, and the Standards. The chief audit executive must periodically review the internal audit charter and present it to senior management and the board for approval.

This also applies to all types of internal audit work as per Attribute Standard 1000.A1 and 1000.C1 respectively which state that: 'The nature of assurance services provided to the organization must be defined in the internal audit charter. If assurances are to be provided to parties outside the organization, the nature of these assurances must also be defined in the internal audit charter.' And that 'The nature of consulting services must be defined in the internal audit charter.' If assurances are to be provided to parties outside the organization, the nature of these assurances should also be defined in the charter. The nature of consulting services should be defined in the charter.

The audit charter may be used in a positive fashion to underpin the marketing task that is discharged by audit management. It can also be used to defend audit services in the event of a dispute or an awkward audit. The charter formally documents the *raison d'être* of the audit function. It is important that all audit departments both develop and maintain a suitable charter. The IIA has issued a statement of responsibilities that covers the role of internal auditing and this document may be used to form the basis of such a charter.

Role of the Audit Charter

The audit charter constitutes a formal document that should be developed by the CAE and agreed by the highest level of the organization. If an audit committee exists then it should be agreed in this forum although the final document should be signed and dated by the CEO. The IIA's attribute standard 1000 covers the purpose, authority and responsibility of internal audit:

> The purpose, authority, and responsibility of the internal audit activity must be formally defined in an internal audit charter, consistent with the Definition of Internal Auditing, the Code of Ethics, and the Standards. The chief audit executive must periodically review the internal audit charter and present it to senior management and the board for approval.

The audit charter establishes audit's position within the organization and will address several issues:

1. The nature of internal auditing This should cover the general concept of auditing and the fact that it comprises the impartial assurance regarding systems of internal control by providing

that they are subject to formal review. In addition, internal audit may provide an associated consulting service.

2. The audit objectives The precise definition of internal audit should be set out. This will be in formal words and include references to the objectives of internal audit. There should be a clear link into organizational objectives and the way that the internal audit role contributes to these. The consultancy-based services from internal audit should be specifically provided for. It may be possible to use the formal definition of internal audit applied by a professional auditing body such as the IIA or CIPFA.

3. The scope of audit work The main areas that internal audit covers should be a feature of the audit charter. Which, as mentioned before, will relate to

- reliability and integrity of financial and operational information;
- effectiveness and efficiency of operations;
- safeguarding of assets;
- compliance with laws, regulations and contracts.

4. Audit's responsibilities It is important that the role of internal audit is clearly set out and that this is distinguished from management's responsibilities. For each of the components of the scope of audit (see above) the expectation of audit's role should be defined. This will include the audit role in respect of coverage of fraud, compliance matters and VFM. On the whole, one would expect management to be wholly responsible for addressing these matters while audit would review the risk management, control and governance systems that ensure these objectives are achieved. It is possible to provide further detail by outlining internal audit's duty to prepare plans and undertake the required work to professional auditing standards.

5. Audit's authority The audit charter will have to refer to the rights of internal audit and the fact that they are confirmed through the charter itself. This will include unimpaired access to all information, explanations, records, buildings and so on that are required to complete audit work. It may be possible to insert a crucial clause that provides that this access be available without undue delay (perhaps within 24 hours). This is because the time factor can be controversial with some of the more difficult audits.

6. Outline of independence No charter would be complete without a clear reference to the concept of independence. This must be perceived as a high profile, prioritized factor that underpins all audit work. While it is necessary in practice to strike a realistic balance, the intention to secure a high level of audit independence will be specifically documented in the charter.

Key Issues

There are several important points relating to the use of audit charters including:

- The charter should be simple and short, preferably contained within a single sheet of paper that will fit on a website screen. One might imagine the charter forming a full colour, 'glossy' document that may appear at audit's reception. As such we may seek to prepare a summary document on one page for presentation purposes, while the actual charter itself may run across several pages. Accordingly the charter must be a short statement of roles and responsibilities

and not a comprehensive description of audit policies and practices that would be very boring to the typical manager. We may go on to suggest that it should convey a basic message and in so doing be perceived as a mission statement that auditors can rally around. The fast pace of the business world does not cater for documents that run to many pages as these will not be read. In fact the fastest growing management skill is the ability to sum up a situation using the minimum number of words and this is now becoming a universally accepted principle.

- The concept of audit independence should be highlighted. The charter must encapsulate the principle of independence as a key feature of the internal audit service. This must jump out at the reader and set out clearly the need to achieve this distance and authority to enable the CAE to discharge the audit role properly. Independence must not appear as a second thought or a minor matter that is expressed simply by saying 'audit should be independent'. What is required is a brief explanation of the importance of having sufficient independence and a hint at how it has been built into the audit service. Furthermore, there may be a mention of fall-back mechanisms where there is any threat to the auditor's objectivity or the ability to get recommendations implemented.
- If senior management in the organization does not support the charter then considerable problems will ensue. The process of developing a formal charter will bring this point to a head. The document will call for a clear position for audit in the organization and the ability to access all work areas. It will also make mention of the importance of recommendations and officers' responsibilities therein. These features may make audit potentially the most powerful section in the organization and bringing these demands to the chief executive will highlight this factor. The organization will get the type of service that it requires. This will vary from a low-level checking function through to a high profile professional service that tackles the most difficult of assignments. The charter represents a statement by the organization that sets the terms of reference and scope of internal audit. This is something that the CAE cannot produce in private but must be a public document signed by the highest level of the organization and widely publicized. It cannot be rubber stamped or simply signed and filed away. It must represent a living policy that is referred to time and time again by both audit and management.
- The reporting process should be briefly described. This should indicate who audit reports to, both in terms of the results of individual audits and for activity reports (e.g. quarterly and annual reports). It is here that the role of the audit committee may be mentioned as there is a clear link between the charter and the committee that raises the status of internal audit. The audit manual will obviously contain much detail on the reporting process from inception through to formalized final reports. This will include clearance procedures and the various management meetings that underpin the negotiation process. It is inappropriate to go into great detail in the charter although it is possible to issue a separate document to managers that sets out how audits are carried out and how the resulting reports are prepared and agreed. This will also explain the role of the audit committee that receives summarized versions of either all or perhaps just the more important audit reports. This is a useful device since there is a view that the audit committee may be somehow spying on managers via the audit process. As such it is as well to explain the role and objectives of the committee forum. One would go on to detail why audit also reports to a higher overseeing body in line with accepted best practice for organizational accountability. Whatever the final formula, the charter should contain a formal but brief statement on reporting that can be expanded on elsewhere.
- Some reference to the auditors' code of ethics may be included in the charter. While the charter may be seen as the authoritative service contract between the organization and internal audit, the code of ethics provides the moral contract that underpins all professional work. Sophisticated concepts such as the requirement for auditors to seek to develop the audit

service with the organization are dealt with through the ethical code, along with many other similar issues. The act of establishing this link between the charter and the code of ethics gives proper organizational recognition to the matters dealt with in the code. As such there is an additional requirement for the auditor to comply with the code, not only to satisfy professional affiliations but also to adhere to corporate policy.

- The requirement that internal audit assume no line responsibilities in the organization should be noted. This is important, since there is much misunderstanding of the real role of internal audit. In the main misguided managers feel that audit checks the output from their systems as the main audit role, which makes them part and parcel of these systems. Audit meanwhile will restate professional auditing standards and argue that if managers do not assume responsibility for ensuring that systems are controlled, then this defeats the key principles of control. No amount of theoretical argument will solve this problem where the rules are not set within the charter. Most managers would state that audit must surely perform in the way the organization requires it to perform, and it is here that the charter becomes an important reference point in such a debate. Again, so long as this specific point is contained in the charter, then the CAE's position is protected. Where this is not the case, there is more scope for misunderstanding.
- The position regarding responsibilities for detecting, investigating and resolving frauds should be clearly established. We have mentioned several times before that the topic of fraud investigations can be a very sensitive matter. In the final analysis internal audit will most probably be the people to investigate such problems and the CAE should see this as extra work for his/her staff. Having said this, it is nonetheless important that the principle of ownership of responsibility is sound. In this way we would seek to make reference to management's duty to prevent, detect and investigate frauds and irregularities. Once set up in the charter, this statement confirms the corporate view that audit only assists managers in solving these types of problems and does not assume wholesale responsibility over and above the advisory role.
- A note regarding the need for full co-operation with the organization's external auditor may also be included. This simply links the two functions and recognizes the need to interact from time to time. It also provides authority to copy what may be confidential reports to the external auditor and not have this act defined as whistleblowing. This can be useful where the CAE tackles a particularly sensitive problem and feels the need to get support from the external auditor. In the worst cases it may be that the organization does not support the line of enquiries that the CAE is pursuing although there are matters that need to be subject to scrutiny and review. The ability to get the external auditor involved in debates that impact on the financial statements can provide an additional layer of comfort for the CAE where there is pressure to abandon or amend the project. Notwithstanding this it is good practice to develop a formal relationship with external audit in the normal course of developing and implementing audit plans.
- The charter should be a statement of basic principles and not a procedures manual. As such, it should be possible to keep it short and to the point. A useful point is to make reference to the audit manual as a way of drawing out the detailed management and operational standards that would direct the audit function. This may be used to give formal status to the audit manual since so long as auditors comply with the requirements of this document, then they can be said to be operating within their agreed terms of reference. If the audit manual is compiled to meet professional auditing standards then this means that the CAE can adhere to quality standards while at the same time conforming to a document that has been formally recognized by the

organization via the audit charter. It is for the CAE to ensure that the audit manual is drafted in a way that promotes an efficient and effective audit service and the audit committee should not interfere with this principle.

- The charter should be formally approved at the highest level of the organization. This sets the tone for all other documents prepared by the internal audit service and creates the authority to perform. The array of documents and policies established for audit should ideally flow from the audit charter in due recognition of this fact. The CAE would seek to prepare three types of documents that help direct and bind the audit service. These will operate as part of the audit manual process, the code of ethics and items that are formally released across the organization. The first two, audit manual and code of ethics, are standards that are set for professional and quality purposes. The third item, publications, expands on the statements contained within the audit charter. To capture this model, we may set out a suitable diagram showing the types of matters that may appear in each category, as an extension of the high-level audit charter as in Figure 5.6.

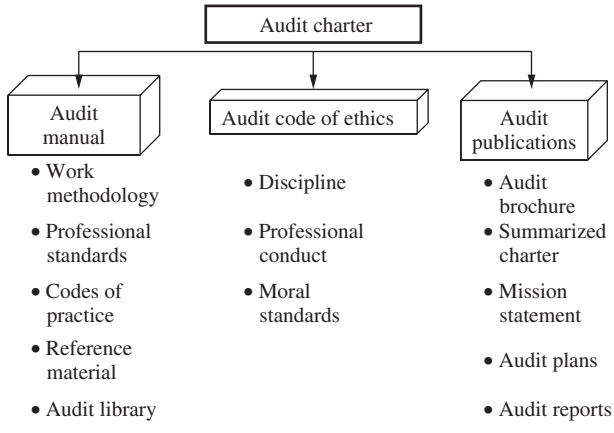


FIGURE 5.6 Standards that flow from the charter.

- The key point that is derived from the above is that a poorly thought-out charter (or for that matter, where there is no formal charter in existence) has a knock-on effect on other standards that are really dependent on the formal authority to discharge an audit service. Where the three main types of documents do not attach to any formal authority they may become mere pieces of paper that can be blown away by a stiff breeze. This is in contrast to the correct position where each document may be defended at all levels in the organization if they are at all challenged.
- As noted, unrestricted access should be agreed within the charter and this should occur at all levels throughout the organization. It is best to stay away from a financial bias and view the organization as a collection of major management systems. Ideally, one might consider adopting a management audit approach that will be able to take on board all areas of the organization. The main point is that this wide scope of audit work should be referred to in the charter so that access is deemed to cover any and everything that may impact on the audit role. This is over and above the basic accounting systems that have been seen by management as the

traditional province of audit. If the auditor arrives at a meeting to discuss the way corporate policy is controlled there should be no resistance from senior managers who perceive this to fall outside the agreed scope of audit work. A simple reference to the charter should enable the CAE to respond to this point, although one would have expected that marketing devices (such as the audit brochure) should have already addressed these types of issues.

- The charter should not require frequent changes as any such alterations will have to go through the same approval process. As such, it should contain statements of general principles that will tend to remain intact over the years. Having said this, it should be updated as and when required. One must remember that internal audit is a developing profession and we would expect changes as the style and emphasis of audit work develop over time. The charter, as a living document that reflects best auditing practice should not be allowed to fall out of date. In one sense it is as well to bring the document before the eyes of corporate management as these people will change with resignations and new arrivals. Again to allow the charter to become a document that was agreed many years ago by people who have since left the organization is extremely unwise. Following this line, one may argue that the charter should be revised, say, annually, although this must not become a process of rejustifying the existence of the audit process each year. The original charter sets up the audit concept while the annual review simply allows for any adjustment to detail that may have become necessary. It is the adjustments that are approved not the entire charter.
- The scope of audit work should include non-audit consultancy work as a direct response to meeting management's needs. It is important to differentiate between audit assurance work and consultancy, which is an additional service. The charter will clearly set out the formal role of internal audit based around the system's work that is performed to discharge the audit role. At the same time authority to perform investigations under the consultancy role should also be agreed and referred to in the charter. The audit manual will obviously explain these two concepts in great detail which in turn will be summarized in glossy brochures released to management. What is needed in the charter is a simple reference to this matter.
- Whatever the expectations implied by the charter, the CAE should ensure that the audit function can meet them. This final point is crucial since great power can readily be agreed but the exercise of this power then has to meet enhanced expectations. Not only does the charter contain a statement of rights but it will also require audit to discharge certain responsibilities against the background of the appropriate professional standards. The audit committee will support and promote audit but will also consider the extent to which they have achieved acceptable standards of work. This acts as a control over the audit function. We can go on to argue that the charter, in turn, also acts as a form of control in setting expectations of the organization that must be seen as a key driving force for the CAE's work.

Structure of the Charter

It is possible to outline a suitable structure for the charter bearing in mind the different models that will be applied by different types of organizations as per Figure 5.7.

The Audit Charter – an Example

Each individual charter will vary depending on the needs of the organization, views of the CIA and type of services offered. We have produced a charter for a fictional company, Keystone Ltd.

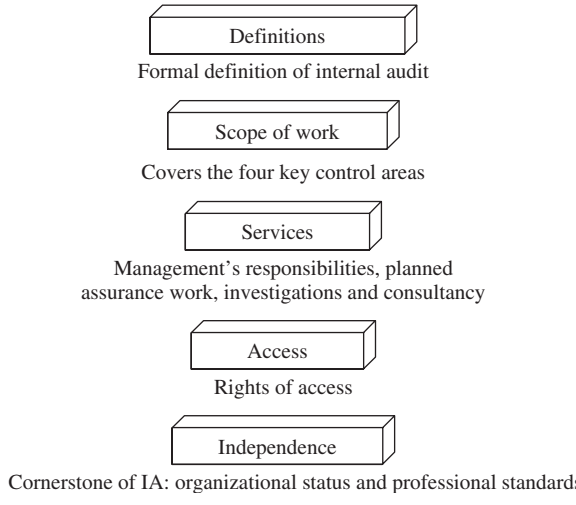


FIGURE 5.7 Structure of the audit charter.

KEYSTONE AUDIT SERVICES – AUDIT CHARTER

This audit charter sets out the role, authority and responsibilities of the internal audit function and has been formally adopted by Keystone Ltd. on 1 January 20xx.

1. Role

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps organizations accomplish their objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes. Internal audit is concerned with controls that ensure:

- reliability and integrity of financial and operating information
- effectiveness and efficiency of operations
- safeguarding of assets
- compliance with laws, regulations and contracts.

2. Responsibilities

Management is responsible for maintaining an adequate system of internal control to manage risks to the organization. Internal audit will provide assurance services to management, the board and the audit committee in terms of reviewing the adequacy of these systems of internal control. Internal audit will also provide a consulting role in helping promote and facilitate the development of effective systems of risk management and internal control. In addition, and subject to the availability of resources, audit will seek to respond to management's requests for investigations into matters of fraud, probity and compliance. Internal audit will provide advice on addressing these problems, which remain the responsibility of management. Furthermore, internal audit shall have no responsibilities over the operations that it audits over and above the furnishing of recommendations to management. The results of consulting and

ad hoc projects requested by management will be used to inform internal audit's position on assurances where appropriate.

3. Plans

Internal audit is required to publish an annual audit plan to the board and audit committee and perform the audits that are contained within this plan, to the standards set out in the audit manual. Annual audit plans will be based on the risk assessments carried out by management and the board and take into account issues derived from the current audit strategy that is approved by the audit committee.

4. Reports

All audit reports will be cleared with the relevant management and once agreed will be copied to the appropriate director, the audit committee and external audit. Management is expected to implement all agreed audit recommendations within a reasonable time frame and each audit will be followed up to assess the extent to which this has happened. The audit committee will be given a summary of audits where agreed recommendations have not been implemented by management without reasonable explanation. The audit committee will also receive a summary of all audits where management have decided not to implement an audit recommendation without reasonable explanation. The overall results of audit work will be reported quarterly to the audit committee (who in turn report to the board of directors). Internal audit is also required to furnish an annual assurance on the state of internal control in the organization.

5. Access

Internal audit has access to all officers, buildings, information, explanations and documentation required to discharge the audit role. Any interference with this right of access will be investigated and, if found to be unreasonable, will be deemed a breach of organizational procedure and dealt with accordingly.

6. Independence

Internal audit is required to provide an objective audit service in line with professional auditing standards (as embodied within the audit manual) and the auditor's code of ethics. To this end it is essential that sufficient independence attaches to this work for it to have any impact on Keystone Ltd. This is dependent on sufficient organizational status and the ability to work to professional standards and the audit committee will undertake an ongoing review of the impact of these two factors.

CHIEF EXECUTIVE ***CHAIR OF AUDIT COMMITTEE***
DATE ***DATE***

The audit charter may be seen as the mission statement of internal audit and a clear definition may be documented to form the basis of later explanations that auditors may apply when describing their role to management. It may also come to the CAE's aid in the event of a dispute with management which is why it should be formulated by the CAE and agreed with the utmost care and consideration.

Giving Internal Audit An Effective Mandate

By Dan Swanson, *Compliance Week Columnist*

Internal auditing's unique position within a company provides management and audit committee members with valuable assistance, by giving objective assurance on governance, risk management and control processes. For internal audit to be effective, however, the mandate of the internal audit function must be clearly defined, agreed to by all stakeholders, and approved by the board. Executive management and members of the audit committee are the two key stakeholders in most organizations, so involving them is critical to ensure the internal audit mandate is balanced and meets the needs of everyone in the company. Also, remember that resourcing is driven by the mandate; that is, an incomplete mandate will lead to inappropriate allocation of resources.

The Mandate: a Critical Success Factor

The authority of the internal audit department is documented in its internal audit charter. An important area to explore first is the role the internal audit department should have: What services should it provide? What should its priorities be? Discussions with members of the audit committee and management should be held to determine what assurance and consulting services are needed. Exploring what internal audit departments at peer companies are doing can also be useful, and helps ensure that the approved internal audit mandate is current with best audit practice.

The internal audit department must support the audit committee's responsibilities, so the committee's charter should be reviewed when defining internal auditing's roles and responsibilities. In fact, an annual ''alignment review'' of the two charters – audit committee and internal audit – is strongly recommended. While the NYSE listing rules require an annual review of the audit committee's mandate, it is silent regarding internal audit. In my view, reviewing both charters every year makes good business sense, and the internal audit charter and the audit committee charter should be mutually supportive and reinforce their critical relationship.

Tackling the Internal Audit Charter

Establishing or updating an internal audit charter isn't always easy. A variety of components need to be developed, and usually a company must go through several iterations of the charter's actual content before striking the right tone. Participation by the entire internal audit department staff – at least the management team of internal audit – is crucial; without involvement, after all, there's no commitment. The overall mission and scope of work should be defined first; one good place to start is an accountability statement for the chief audit executive. Companies should also discuss issues of independence; for example, who sets the scope of internal audit projects, and to whom should the chief auditing executive report? (Another quick tip: Including a statement in the charter about the auditor's open and free access to all information across the organization can save your auditors a lot of grief.)

The responsibilities of the department – what the function is and is not accountable for – comprise the majority of an internal audit charter. Including a standard of performance is also common, to delineate what standards should be used by the internal audit function in the performance of its work. The most common standard is the International Standards for the Professional Practice of Internal Auditing, as promulgated by the Institute of Internal Auditors. Once a draft internal audit charter has been developed or updated, it needs to be reviewed by the stakeholder groups, and there are many different ways to get a draft charter approved and published. One common approach is to set aside time during an off-site meeting of internal audit staffers and management – with key executives like the CEO and CFO visiting – for the review and finalization of the audit charter. With Web-based interactive technology, the virtual sharing of the draft charter with all the stakeholders has become very popular, as it enables open-threaded discussions to take their course, and can increase acceptance levels. At smaller companies, a few key executives at a single staff meeting can finish the document in a morning. Development of an effective audit charter generally involves a combination of all of the above methods, plus others.

Revisit the Mandate Annually

The mandate of the internal audit department – defined in the internal audit charter – assists the department in performing its work because management and others are able to understand clearly what internal audit is charged with doing, and what they are accountable for. The audit charter is also a great communication vehicle for internal audit to discuss its services and priorities with clients and stakeholders. In top-tier organizations that take governance seriously, presenting the approved internal audit mandate to the board or management committee is a common way of presenting the future: the goals of internal audit, the value the function brings to the organization, and its priorities and plans. This is also an excellent way for internal audit to obtain management's agreement and feedback on the internal audit plans.

Directors must satisfy themselves that the mandate of internal audit is appropriate and that the internal audit function will contribute to the organization's efforts. The dialogue between management, the audit committee, and the leadership of the internal audit function regarding the mandate is one of the keys to an internal auditing department's long-term success.

An approved and published internal audit charter is not the end of implementing an effective internal audit function; it's more like the end of the beginning. Really, the audit mandate is revisited with every new audit project as employees ask, ''Why are we doing this?'' Having a clear, approved charter makes answering that question much easier.

Reprinted from *Compliance Week*. This article was originally published in Compliance Week. Reproduced by permission of Compliance Week. All rights reserved.

5.4 Audit Services

The role of internal auditing is wide. Within the context of improving risk management, control and governance processes, the type of work undertaken to add value to an organization will

vary greatly. Organizations with rigid regulatory requirements in an industry where scandals are common may find that compliance reviews are the best way to add value to the business. Enterprises in rapid growth sectors where speed in delivering new products is the key to success may find that consulting advice on controlling programmes and projects may be the most appropriate value add proposition. Public bodies in developing countries may want their audit effort directed at helping to build better controls and deal with corruption issues. Companies and bodies that are embarking on a long-term reform programme may want their auditors to help build a capacity to self-assess risk and controls in line with awareness events and facilitated self-assessment programmes. Organizations that are spread across the world and linked by associates, joint ventures and partnering deals may want their auditors to keep head office informed about local systems and arrangements and whether risks are being managed properly. It all depends on the context and best use of resources. Internal audit shops that focus on the corporate governance arrangements, rather than take on any work that comes its way, will tend to have a better direction. The remit is the audit charter, the parameters are the professional standards while the context is the success criteria that is set by the organization. Within these factors will fall the range of audit products that are on offer. These may include one or more of the following possible interpretations of the audit role. Note that the following are listed internal audit services selected at random from various websites that feature internal audit shops from both private and public sector organizations:

- cyclical audit (stock petty cash payroll);
- investigations into specific problems;
- responding to requests by management;
- operational efficiency and effectiveness reviews;
- internal control reviews;
- fraud investigations;
- compliance reviews;
- reviewing controls over revenue, contracts administration and operational expenses;
- acting as a contact point for allegations of fraud, waste and abuse;
- information system reviews;
- financial and compliance audits;
- performance audits;
- internal control reviews and testing poor areas;
- investigative audits into reported irregularities;
- verify assets and review safeguards;
- evaluation of reporting systems and procedures;
- cost saving reviews;
- review of administration and accounting controls;
- financial and performance audits;
- revenue audits;
- management studies into cost savings, problems in technical support and performance;
- special reviews of projects;
- control self-assessment facilitation;
- environmental audits;
- auditing the change management process;
- operational audits;
- computer audits;
- control self-assessment questionnaire design and analysis;

- issuing guidance to staff on internal control;
- value driven internal consultancy, acting as change agents;
- business process analysis;
- business risk assessments;
- quality advocates and reviews;
- providing measures to strengthen mechanisms to achieving objectives;
- evaluation of corporate governance processes;
- working with management on their risk management practices;
- advising clients on risk exposures and measures to remedy;
- review risk management arrangements;
- provide practical solutions and supporting management in implementing them;
- participating in major information systems projects;
- reviews to improve quality of management processes;
- communicate risk information to clients;
- operational auditing (or management audits);
- financial system audit, accounting and financial reporting;
- compliance auditing on adherence to laws, regulations, policies and procedures – concentrating on improved controls to help compliance;
- computer auditing during development stage;
- audit approach determined by discussion with management but final result remains an internal audit prerogative;
- advice to managers when making changes to procedure;
- training in risk and control awareness;
- provision of independent assurance on internal controls;
- general advice and guidance on control related issues;
- operate follow-up system for outstanding audit recommendations;
- evaluate action plans made in response to audit recommendations;
- liaison and joint projects with external audit;
- special projects as requested by management;
- management reviews of new or existing programmes, systems, procedures;
- control consciousness seminars;
- recommendations for enhancing cost-effective control systems;
- monitoring financial information and reporting results;
- reviews of fixed assets, cash receipts, budgets, purchasing and accounting routines;
- surprise audits over cash funds, accounting records, employee records, observation of operations and inventory records;
- accountability and fraud awareness training;
- projects to improve quality of information or its context for decision making;
- reviews of e-commerce arrangements and security;
- audits of internal control structures, efficiency and effectiveness and best practice;
- safeguarding assets (and information) using verification of asset registers, inventories and the adopted security policy.

There is clearly an abundance of related services on offer from the many internal audit shops in existence. Some built around the compliance model and others focusing more on consulting projects. There is one word of warning that should be included here to close this section of the chapter. This comes from extracts of an article by William Levant, who has a view on the traditional cyclical audits that many audit shops hold dear to their hearts:

> It's no longer good just to do cycle-based audits. And it is also no longer adequate to do risk based audits . . . bringing risk consulting and IA closer together. IA exclude the executives from the risk planning process . . . IA tackle compliance and the framework for controlling risk. Pressure to cut costs, increase performance and account for activities to shareholders. Auditor core competencies – corporate governance and risk consulting, business transactions and processing, technical IT skills . . . Some internal auditors get far too hung up on the notion of independence. If you are working within an organization, your views cannot be considered independent. The key issue is about being objective.[4]

The IIA definition of internal audit can be used as a framework for developing appropriate audit services. The question to ask is: How can we best contribute to risk management, control and governance services through both our assurance and consulting roles? The answer will help define the types of services that should be on offer. Do all the above audit services add value to an organization? To help answer this question we can turn to the advice from an IIA Task Force consisting of Jack L. Krogstad, Anthony J. Ridgey and Larry E Rittenberg:

> Ample evidence shows that most audits, including compliance audits, add value to the organization because they keep management informed about the effectiveness of its control structure. Nevertheless, in today's highly competitive and cost-conscious world, the Task Force asserted its view that management requires everyone in the organization to contribute value, and that there is a need to market more aggressively the value-adding services that internal auditors can provide . . . The Guidance Task Force maintains that the profession's future viability rests on maintaining high quality services throughout its ranks. They argue that achieving universal compliance with standards that lead the profession thereby becomes a symbol of distinctive quality in the marketplace.[5]

What Internal Auditors Want

By Dan Swanson, *Compliance Week Columnist*

In my line of work, I'm often asked exactly what internal auditing is supposed to be. According to the International Standards for the Professional Practice of Internal Auditing, the answer is pretty straightforward: ''Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations.''

You might want an answer more expansive than those 19 words. So this month, let's take a step back from the fine points of executing internal audits, to re-acquaint ourselves with what internal audit is and how you can make it helpful to your job. Internal auditing provides opportunities for companies to improve based on independent analysis and advice. Internal audit also helps the board and senior management monitor the organization. To preserve the integrity and independence of audits, auditors maintain a delicate balance between offering advice (mainly consulting services) and providing opinions about a process, system, account balances, or other subject matter (assurance services).

The size and complexity of internal auditing functions are as diverse as the range of operating environments, risk appetites, and business and audit objectives that a company can have. The scope of audits can also vary from project to project within a company, depending on an auditor's focus (for example, on high-risk business processes, or key management and technical controls). Ensuring appropriate audit focus is one of many reasons that management should communicate with auditors, and vice versa, early and often for every audit project.

What Does Internal Audit Do?

Internal auditing provides strategic, operational, and tactical value to an organization. For example, when evaluating information security, the internal auditor informs the board and management about whether:

- business units understand the importance of security and are adhering to policies;
- key information assets and systems are sufficiently secure;
- programs exist to update and strengthen safeguards constantly against internal and external security threats; and
- the organization's policies are reasonable.

The internal auditor might also independently validate that the organization's information security efforts are proactive and effective against current and emerging threats. To provide this level of assurance, the internal auditor may compare current organizational practices with industry practices and regulatory guidelines. Notably, auditing provides only a reasonable level of assurance. Auditors cannot provide an insurance policy against every possible fault or deficiency, particularly regarding activities that cannot be totally controlled, such as collusion or management override.

What is Management's Role?

An internal audit engagement typically has three phases: planning, testing, and reporting. Management has a vital role to play in each one. During planning, senior management should first focus on the audit plan (the auditor's ''roadmap'') and ensure that business managers understand audit's purpose, focus, and approach. An open, positive discussion with the audit team regarding these defining factors helps both management and the audit team communicate their expectations up front.

Audit planning should focus on critical or sensitive risks, but all risks should be considered. To this end, active involvement by management in audit planning can contribute to the overall success of an audit. Management should ensure that things they consider to be risks are addressed by the audit plan. Both the auditor and management should be identifying areas of risk. Management should also discuss the evaluation criteria auditors will use to assess the activity being audited. Lastly, managers and auditors should broadly discuss planned audit testing, although auditors must have the authority and discretion to select tests they deem appropriate and the transactions being audited.

During testing, management facilitates the auditors' access to appropriate people, systems, and facilities. Management should confirm the presentation of the facts by the internal auditor, ensuring that the auditors have considered all the information available. The audit team leader and senior executives of the areas being audited should meet regularly – perhaps even weekly, and at a minimum at least once during each audit phase – to discuss audit progress, identified issues, and potential actions. An open dialogue between senior members of both management and the audit team does much to avert misunderstandings and resolve disputed findings before the audit team issues its draft report. The audit team should communicate critical findings to management as early as possible, even outside of the established meeting schedule. These findings may also be reviewed during regular meetings, but prompt notice is necessary and usually appreciated.

During reporting, the internal audit team communicates its analysis and recommendations. Management receives and reviews the findings, develops corrective actions, and may even begin implementing changes. Management should ensure the presentation of the findings is appropriate. They should also determine whether or not they are willing to accept the level of risk identified. If not, they should develop a realistic action plan with specific goals and timelines. And managers shouldn't agree to recommendations that they can't actually do. (Too often I see management agreeing and, in the same breath, saying: ''We will put in a business case to get the necessary resources.'' If they don't have the resources, they're not in agreement.) If, on the other hand, the company is willing to accept the risk, this should be clearly stated.

The Bottom Line

Audits exist to assess how well a business unit meets the performance goals of the organization, as dictated by the CEO, CFO, board, investors, and others. Accordingly, management's goal is to demonstrate how well operations, controls, and results meet the needs of the business. During audit planning, managers should work with the auditors to ensure the audit scope, goals and objectives are appropriate. Thus, prompt response to the auditors' requests for information and records throughout the audit process – planning, testing, and reporting – is for the benefit of the business, not its auditors. Auditors exist to provide the board and senior management with an objective, independent assessment of a business unit or program (such as information security), including what they see as key opportunities for improvement. To prepare their opinions and conclusions, auditors need to review evidence of the risk-management efforts and assess performance. If managers are able to demonstrate performance and show that accountability has been established and effectively discharged, it will result in a positive audit report. It's that simple.

The ultimate goal of management throughout the audit process should be to demonstrate that their efforts meet the expectations of the CEO, board of directors, and investors. Likewise, the auditor's requests should be aligned with these overarching needs; that is, to support responsible performance within a sound and ethical business environment. Accordingly, auditors and managers should work to help each other reach common goals – auditors striving to earnestly, honestly, and competently assess program effectiveness, and management working to help auditors complete valid assessments. In that vein, auditors always look for sound management practices. Always remember that managers, not auditors, are responsible for defining and implementing solutions to issues found in the audit. Thus, it is in everyone's best interest to have a cooperative, collaborative audit process that respects the independence and discretion of all participants. Auditors should listen to management. And for its part, management should encourage staff to be open and honest with auditors. Have you talked with your auditor lately?

Reprinted from *Compliance Week*. This article was originally published in Compliance Week. Reproduced by permission of Compliance Week. All rights reserved.

5.5 Independence

All definitions of internal audit contain the word 'independence' and this is an important component of the audit role. It is both a concept and an ideal. One could assume that since internal audit is located within the organization it cannot be independent. The counterargument suggests that internal audit has to be totally independent, or it has little use. The real position falls somewhere in between. There are degrees and a quality of independence that has to be earned to ensure that audit is sufficiently distanced from the particular operation being reviewed. IIA standard 1100 covers independence and objectivity:

The internal audit activity must be independent, and internal auditors must be objective in performing their work.

Interpretation:

Independence is the freedom from conditions that threaten the ability of the internal audit activity or the chief audit executive to carry out internal audit responsibilities in an unbiased manner. To achieve the degree of independence necessary to effectively carry out the responsibilities of the internal audit activity, the chief audit executive has direct and unrestricted access to senior management and the board. This can be achieved through a dual-reporting relationship. Threats to independence must be managed at the individual auditor, engagement, functional, and organizational levels.

Objectivity is an unbiased mental attitude that allows internal auditors to perform engagements in such a manner that they believe in their work product and that no quality compromises are made. Objectivity requires that internal auditors do not subordinate their judgment on audit matters to others. Threats to objectivity must be managed at the individual auditor, engagement, functional, and organizational levels.

Standard 1110 deals with the need to achieve a degree of organizational Independence:

The chief audit executive must report to a level within the organization that allows the internal audit activity to fulfill its responsibilities. The chief audit executive must confirm to the board, at least annually, the organizational independence of the internal audit activity.

1110.A1 – The internal audit activity must be free from interference in determining the scope of internal auditing, performing work, and communicating results.

1111 – Direct Interaction with the Board

The chief audit executive must communicate and interact directly with the board.

1120 – Individual Objectivity

Internal auditors must have an impartial, unbiased attitude and avoid any conflict of interest.

Interpretation:

Conflict of interest is a situation in which an internal auditor, who is in a position of trust, has a competing professional or personal interest. Such competing interests can make it difficult to fulfill his or her duties impartially. A conflict of interest exists even if no unethical or improper act results. A conflict of interest can create an appearance of impropriety that can undermine confidence in the internal auditor, the internal audit activity, and the profession. A conflict of interest could impair an individual's ability to perform his or her duties and responsibilities objectively.

While standard 1130 addresses the need to deal with any impairment to independence or objectivity:

If independence or objectivity is impaired in fact or appearance, the details of the impairment must be disclosed to appropriate parties. The nature of the disclosure will depend upon the impairment.

Interpretation:

Impairment to organizational independence and individual objectivity may include, but is not limited to, personal conflict of interest, scope limitations, restrictions on access to records, personnel, and properties, and resource limitations, such as funding.

The determination of appropriate parties to which the details of an impairment to independence or objectivity must be disclosed is dependent upon the expectations of the internal audit activity's and the chief audit executive's responsibilities to senior management and the board as described in the internal audit charter, as well as the nature of the impairment.

There are several other aspects of the main 1130 standard that should also be noted:

1130.A1 – Internal auditors must refrain from assessing specific operations for which they were previously responsible. Objectivity is presumed to be impaired if an internal auditor provides assurance services for an activity for which the internal auditor had responsibility within the previous year.

1130.A2 – Assurance engagements for functions over which the chief audit executive has responsibility must be overseen by a party outside the internal audit activity.

1130.C1 – Internal auditors may provide consulting services relating to operations for which they had previous responsibilities.

1130.C2 – If internal auditors have potential impairments to independence or objectivity relating to proposed consulting services, disclosure must be made to the engagement client prior to accepting the engagement.

The Meaning of Independence

Independence means that management can place full reliance on audit findings and recommendations. *Brink's Modern Internal Auditing* makes clear the crucial role of audit independence: 'internal

audit is the one function in the modern organization that is completely detached from both the operational components and functional staff groups'.[6]

There are many positive images that are conjured up by this concept of independence:

1. Objectivity Behind this word is a whole multitude of issues that together form a complex maze. The main problem is that the whole basis of objectivity stems from a human condition of correctness and fair play. Any model that involves a consideration of the human condition have to deal with many psychological matters, and at times irrational behaviour. Although objectivity is located in the mind, it is heavily influenced by the procedures and practices adopted. The ACCA guide to *Ethics and the Accountant in the Public Sector* defined objectivity in the following way: 'Objectivity can be described as a state of mind which allows the individual to make judgements, based upon all the available evidence relating to the situation, in a state of emotional and psychological detachment from the situation or decision.'[7]

2. Impartiality Objectivity may be seen as not being influenced by improper motives while impartiality is not taking sides. The question of impartiality is important because there is a view that internal audit, like all other units, will work in a politically advantageous way. This may result in audit taking the side of the most powerful party in any work that impacts on the political balances within an organization. If this is allowed to occur unchecked then the audit evidence that supports any audit report may be secured with a view to assisting only one side. An absence of impartiality will undermine the audit process. If audit plans are changed, reports withdrawn and audits aborted because this suits certain parties in the organization, this reputation will stay with the audit function and give it a poor image.

3. Unbiased views When an audit report states that 'the audit view is . . . ' this should provide a comment on the state of internal controls. When used to provide an advantage for the audit function, credibility is risked. The other aspect of audit bias is where certain officers/sections have been earmarked as 'poor, uncooperative or suspect . . . ', we go into an audit looking for any material that supports our original contentions. If taken to the extreme, the audit function will become a hit squad, conjuring up cases against people it does not like. It is difficult to build professional audit standards using this model. In the UK, the year 2002 saw regular strikes by firefighters against the background of a review of their pay and working practices. The importance of the perceived impartiality of the review team is essential to ensure all sides buy into the results of the review. In the case of the firefighters this goodwill was not present: 'Fire Unions Call for Member of Pay Review to Quit: Firefighters' leaders last night called for the resignation of a member of a Whitehall pay review team after claiming he had privately admitted the three man inquiry would reject the union's pay claim for £30,000 a year.'[8]

4. Valid opinion Readers of audit reports require the auditors to complete work to professional standards with the audit opinion properly derived from this work. This opinion must make sense having reference to all relevant factors. The audit role is not to please nominated parties or simply maintain the statusquo; it is to present audit work in a professional and objective manner. The temptation to keep certain individuals happy may well result in a distorted audit opinion which in turn will make the underlying audit work unreliable. Managers will issue hundreds of reports during the course of their careers, each taking a stance that is derived from their position within the organization. Internal audit on the other hand depends wholly on a reputation for reviewing an area, or performing an investigation, and producing an opinion that is valid. This is not to suggest that this opinion will be supported by all levels of management, but it should be accepted as a fair representation of the facts.

5. No spying for management Professional objectivity means that audit does not fall into the trap of acting as spies for management, particularly where managers feel that their staff are not performing. Most general problems with staff can be related to a failure by management to install effective controls and this is a point that the auditor will return to time and time again. The latest definition of internal audit suggests that audit serves the organization as a whole rather than targeting specific officers. This means that the welfare of the organization is paramount as the audit role rises above the in-fighting that goes on in both private and public sector bodies. There is an issue surrounding the provision of audit consultancy services that makes this a complicated area which is dealt with later.

6. No 'no-go' areas There are senior managers who adopt a particularly aggressive stance to managing their areas of responsibility. All outsiders are treated with great suspicion. In fact there is a correlation between professional incompetence and this threatening posture, i.e. the less able the manager the more aggressive he/she becomes. If this results in certain areas being deemed out of bounds to internal audit then this means that audit's independence is impaired and they will have a lesser role. If audit can be kept away from certain areas then this restricts the audit field, and if this trend is allowed to continue it could set a damaging precedent. The net result may be that the audit field becomes relegated to defined parts of the organization only. This is playing at auditing far removed from the demands of any professionally based audit practice.

7. Sensitive areas audited To achieve its full status internal audit must be able to audit sensitive areas. Unlike the no-go areas, this potential barrier arises where the necessary skills and techniques are not available to the audit unit thus making it impossible to cover high-level areas. Where the audit scope is set within basic accounting systems for low-level checking, little important work can be undertaken and audit independence will not have been secured.

8. Senior management audited There is a view that system controls are primarily located within the management processes that underpins the operations. Where audit fails to incorporate this factor into the scope of audit work, a great deal will be missed. The problem is that managers may not wish to be audited, particularly where this exposes gaps in their responsibility to establish sound controls. The CAE will have a quiet life where he/she works only at a detailed operational level and ignores the whole management process. Again this restricts the audit role and so adversely impacts on the auditor's independence.

9. No backing-off We do not expect auditors to back down without a valid reason when confronted by an assertive manager. This is not to say that auditors march unchecked across the organization, unaware of any disruption they might be causing to front line operations. It does, however, mean that they will pursue audit objectives to the full in a diplomatic and professional manner. If this is not the case then audit will be vulnerable to criticism from all sides. Audit reports would then reflect what managers allowed the auditor to do rather than the work required to discharge the terms of reference for the audit. In this instance audit can claim very little real independence.

The above provides a foundation for the audit practice at the heart of the audit role. This distinguishes it from management consultancy and other review agencies who provide professional review services but only to the terms of reference set by management. These factors must be in place for the audit function to have any real impact on the organization. If managers are able to pick and choose which audit reports to believe, then this represents a major flaw in the audit

service. It will eventually lead to its downfall, as well as a failure to meet professional internal auditing standards. An example illustrates the importance of audit independence and the dangers inherent in 'fixing things':

> A large local authority administered ten cash offices spread around the area for local residents to pay their council tax, rent and other bills. Senior management commissioned a manager to perform a comprehensive review to determine how the cashiering service could be improved and made more efficient. The terms of reference were set around a future strategy to sharpen and focus the service to meet the needs of the residents. Half way through the project, the reviewing manager realised that the senior management team had a confidential plan that involved closing three of the offices as soon as the review was completed. Pressure was then put onto the reviewing manager to find some evidence to justify this decision.

Factors Affecting Independence

Since independence is achieved in degrees, there are many factors that impact on the acquired level of independence:

- Where internal audit is too closely involved in the design of systems, it becomes difficult to stand back at a later stage and audit the same system. People naturally feel their work is correct and of a high standard. There are few who are able, at a later stage, to criticize their own efforts, however objective they may claim to be. Systems designers take on some of the ownership of these systems which necessarily rules them out as independent systems assessors. All systems designed by audit will have to be taken out of the audit field thus restricting the scope of audit coverage. The internal audit role in systems development may mean that audit becomes responsible for the new system. The definition of professional audit services hinges on an agreed model where management is responsible for their systems and systems controls. Excessive involvement in systems design will interfere with this concept and locate responsibility with the auditor who will have to make recommendations to himself/herself whenever reviewing a particular system. Any form of independence in this instance would be a non-starter. An Information Systems Auditing Guideline prepared by Information Systems Audit and Control Association is directed at specialist information systems (IS) auditors and sets standards for dealing with non-audit work:

  The IS auditor is to be independent of the auditee in attitude and appearance. The non-audit role, in general, involves participation in the IS initiatives and IS project teams in working and/or advisory/consultative capacities on a full-time or part-time basis. Such non-audit roles are an important part of the IS auditor's contribution to the education and training of other members of the organization. They enable IS auditors to use their expertise and knowledge of the organization to provide a unique and valuable contribution to the efficiency and effectiveness of the organization's IS investment. They also provide opportunities to raise the profile of the IS audit function and to give IS audit staff valuable practical experience. Where the IS auditor has been involved in a non-audit role in an IS initiative and an audit is subsequently/concurrently performed of that initiative or the related IS function, recommendations and conclusions arising from that audit may be perceived by the recipients as not objective. In this situation, the perception may be that both the independence and the objectivity of the IS auditor have been impaired by the non-audit involvement. The IS audit charter should establish the mandate for the IS auditor to be involved in non-audit roles and the broad timing and extent of such roles.[9]

- Where internal audit is overfamiliar with the client one may view its work as potentially biased by the relationship. There is a view that auditors should seek to remain outside the normal free associations between managers and officers who will strike up informal relationships. Two points addressed later are the audit role in providing consultancy services and the need to avoid a perception (as well as the reality) that audit has close ties with defined managers such as to impair objectivity. An extreme example would be where an auditor has an intimate friendship with a manager although the relationship problem would apply wherever audit has provided assistance to particular managers.
- Conflicts of interest can arise where the auditor cannot stand back from the system. This can happen when the auditor has developed a close social relationship with the manager of the operation under review. The ability to employ good inter-personal skills is a clear advantage to the performance of audit work. however, where, this entails forming close friendships, one risks many subsequent disadvantages that outweigh the original benefits. A carefully formulated and implemented code of conduct is essential in dealing with this complicated subject.
- The practicalities of the situation may make it difficult to preserve independence. Where there is no information systems auditor available, it is difficult to provide an effective input into this area. One aspect of independence is based on a wide scope of audit coverage across the organization. Where this is impracticable the audit impact will suffer accordingly. As such the CAE is charged with formulating a clear strategy to counter all problems that impair the ability to provide an efficient audit service. We need to refer again to standard 1130 for guidance on any impairment to independence or objectivity:

  > If independence or objectivity is impaired in fact or appearance, the details of the impairment must be disclosed to appropriate parties. The nature of the disclosure will depend upon the impairment.

  Impairments to independence may include problems regarding issues such as:

  - scope
  - access
  - work schedule
  - audit procedures
  - staffing plans or budgets.

- Where internal audit reports to the FD, a careful approach has to be negotiated to secure the degree of independence that promotes good audit work. This point is dealt with later.
- Rotation of auditors between assignments gives a fresh eye to periodic audits and avoids the auditor becoming too involved with the system under review. It is not necessarily the relationship with the operational staff in question that is the issue. It is linked more to the level of boredom and sameness that creeps in where the same audit area is tackled again and again by the same person. This is not to say that one cannot assign specific parts of the audit field to specific auditors so that a degree of expertise can be acquired.
- Gifts provided by the client can create obvious problems and firm audit policies must be provided for this matter. The position is not always wholly clear since free drinks, lunches and other minor perks may be part of the culture, with constant refusal causing embarrassment to both sides. There is always a balance to be struck between two extremes as shown in Figure 5.8.



FIGURE 5.8 Receiving gifts.

The real issue here is not so much the value of any perks received as part of working for an organization. It is related more to an outsider's perception if the internal auditor is seen to be accepting favoured hospitality from the client. Where auditors have recently come from a particular operation, it is advisable that they are not involved in auditing this area for a period of time during which they might be assimilated into internal audit. Where an auditor is due to leave internal audit and assume a line role in a particular operation, again they should not be party to audit work in the same area. IIA Standard 1130.A1 and Practice Advisory 1130.A1-1 deals with assessing operations for which internal auditors were previously responsible and this guidance suggests that:

> **1130.A1 –** Internal auditors must refrain from assessing specific operations for which they were previously responsible. Objectivity is presumed to be impaired if an auditor provides assurance services for an activity for which the auditor had responsibility within the previous year. Persons transferred to, or temporarily engaged by, the internal audit activity should not be assigned to audit those activities they previously performed or for which they had management responsibility until at least one year has elapsed. Such assignments are presumed to impair objectivity, and additional consideration should be exercised when supervising the engagement work and communicating engagement results.

In terms of working relationships, there is in fact a dilemma felt by some less experienced auditors. Here they wish to perform an objective audit but also want to impress the client with a friendly and congenial approach. Striking up a positive working relationship is always encouraged but this should not be at the expense of professionalism in an attempt simply to please the client. Breaking these cosy relationships is generally recommended so that both sides may maintain a sense of proportion in performing their respective roles. Again clear policies on this matter are required. The policy of talking to management and incorporating their needs into the project terms of reference creates a positive process but may be manipulated to lessen the level of independence. One would accommodate management's views but only to an extent, so as not to alter the original terms beyond recognition. We can extend this argument to cover those audit departments that have assumed an almost pure consultancy role responding fully to client requests rather than undertaking planned audit work. The difference between consultancy and audit must be fully recognized by the CAE when designing the type of audit services on offer. When discussing factors that affect independence we must move from the position of deciding if we do or do not have independence. The true position is that an idealistic stance cannot be held onto at all costs. The practicalities of each individual case will mean that it merely has to be sufficient to support good audit work. What is important is that the many barriers to acceptable levels of independence should be recognized and addressed via the adopted audit philosophy.

The Three-Component Model

Mautz and Sharif[10] tackle external audit independence through three fundamental components:

1. **Programming independence** – Here the auditor is free to define how the selected areas will be audited and what procedures will be applied.

2. **Reporting independence** – The right to report the full facts is seen as an important aspect of independence.
3. **Examining independence** – External auditors should have freedom to examine all areas that affect the financial accounts.

We have touched on the problems where internal audit is too immersed in the organization's operations and cannot stand back and audit them. The acid test is:

> if internal audit were to be removed, part of the organization would not grind to a halt.

This is excellent theory but does create secondary problems where the organization does not fully understand the audit role thus making the audit function vulnerable. If this is the case, audit will be subject to a strong temptation to adopt a consultancy role and become part of the day-to-day controls so that its absence would be noticed immediately. It is important that internal audit is seen to be independent. While most accepted that internal audit was independent of line managers, these same managers tended to view the auditors as intimately linked to senior management and in fact could not be independent from them. Operational management may adopt a more severe view of the internal auditor and consider them to be management spies who are not prepared to criticize senior management failings. Independence must not only be earned but must also be carefully managed.

Courtemanche on Independence

Courtemanche includes a chapter on independence in his book.[11] He feels that the auditor's style and approach to work affect the degree and quality of independence that is secured. Where the auditor loses support from management, the status, scope and profile of the audit function will decline. Courtemanche discusses four styles of auditing that are akin to adopted audit philosophies:

1. The outsider The auditor represents an outside interest with a regulatory role in the organization. There is no recognition of the goals of the organization and the approach becomes self-limiting with management restricting audit to those limited areas where it can be useful.

2. The manager by proxy The audit role is as an agent for senior management and a special status is therefore acquired. After a while resentment builds up among auditees and pressure is applied to senior management. The tendency is then to restrict the audit role to where they can do least harm to morale.

3. The autonomist This is the worst situation, where the auditor is self-answerable and not to management or an outside regulatory agency. The auditor possesses a special wisdom and attempts to impose on the organization regardless of suitability. The ideals may be engineered to meet managers' requirements for a while but will eventually break down when it becomes clear that auditors report to no one but themselves. This illusion of independence is quickly lost when management withdraws its support.

4. The absolutist The auditor distorts the admirable qualities of honesty and integrity to 'tell it like it is'. The auditor then proceeds to spread trouble and discord throughout the

organization, rejecting all compromise until management's support wears down. The auditor has no professional base or leadership qualities, just a nagging insistence on rightness and the audit role will be restricted by management.

Courtemanche concludes that audit is not simply independent from management but that their independence is in fact dependent on management's support. He sees independence as based on a constructive auditor style while managing the following components:

- access
- freedom to report
- responsiveness (by management) to audit findings
- diligence in performing work
- objectivity and professionalism.

The Rittenberg Model

An important model of audit independence that incorporates all the main ingredients was devised by Rittenberg.[12] The model is divided into two main sections: the organization and the individual. Factors relating to the individual auditor are subdivided into economic and mental:

1. Organization This deals with the position of audit within the organization and covers all relevant factors including reporting levels, top management support, audit committees and the audit charter.

2. Economic These factors relate to the management of the audit department and include policies on designing systems, staffing the audit function, ethics, time restrictions on work and supervisory review.

3. Mental state Factors in this category should ensure that the auditor does not subordinate his/her judgement as required by the standards. The important areas are personal attributes, objectivity, competence and professionalism in providing audit services.

Independence is a complicated issue with many features that must be both considered and properly managed. The two main features may be subdivided into various subsidiary categories giving a much wider view of independence.

A Working Model

Based on research it is possible to formulate a working model for assessing the level of independence. A number of components are considered and one works out the desirable, feasible and actual points on a continuum and then estimates how far one is from what is feasible. This model has been used by Keith Wade who sees the main factors as:

1. Position within the organization The higher one is located within an organization, the greater the ability to offer an independent audit service. The status of each auditor is affected by the seniority of the CAE and where this is not on a high enough level one will only be able to pay lip service to the concept of independence. Furthermore it may be extremely difficult for an auditor to liaise with senior management where he/she is of a much lower grade. The imbalance may impair the auditor's ability to defend the audit view if required.

2. Reporting line The people who are ultimately concerned with the auditor's conclusions concerning the state of controls in specific operations and generally throughout the organization will impact on the level of independence achieved. The ability to resort to the most senior level of the organization when required gives the audit function power which promotes audit objectivity. This access to the formal power structure need not ever be used in practice so long as it is clearly available if needed.

3. Scope of work An ability to address risk and control concerns at the highest level in the organization is a major hallmark of audit independence. This must not only be built into the audit charter but must also be put into practice. A narrow definition of internal audit steeped in basic accounting systems is totally inadequate. The applied audit model must be based around professional definitions that view controls as all measures designed to assist the organization in achieving its objectives. When complemented by a top-downwards approach to control, this allows one to audit the corporate process itself.

4. Level of audit resources With all the best will in the world it will not be possible to achieve an independent audit coverage if the necessary resources are not in place. The right numbers and grades of auditors must be established to discharge a professional audit role. The requisite numbers will depend on the audit strategy, formal audit plans and the adopted approach to work. High-level professional audit work can only be carried out by high-level professional auditors.

5. Freedom from line operations This is very important. Most audit units have now moved away from direct line functions such as certifying contractors' interim and final accounts before payment. However, a new trend has arisen where audit departments seek to discharge management's responsibilities for designing suitable systems and guarding against frauds. This results from mixing consultancy-based work with audit work so that the lines of responsibility become blurred. Management no longer needs to think about the adequacy of their control systems as this role has been passed over to audit. These systems have no real owners and so drift into disrepair. The consultancy debate is outlined later. This vexed issue has been the subject of IIA Practice Advisory, 1130.A2-1: Internal Audit's Responsibility for Other (Non-audit) Functions. The standard 1130.A2 states:

> Assurance engagements for functions over which the CAE has responsibility must be overseen by a party outside the internal audit activity.
>
> While the advisory 1130.A2-1 Internal auditors are not to accept responsibility for non-audit functions or duties that are subject to periodic internal audit assessments. If they have this responsibility, then they are not functioning as internal auditors.

When the internal audit activity, CAE, or individual internal auditor is responsible for, or management is considering assigning, an operational responsibility that the internal audit activity might audit the internal auditor's independence and objectivity may be impaired. At a minimum, the CAE needs to consider the following factors in assessing the impact on independence and objectivity:

- Requirements of the Code of Ethics and the *Standards*.
- Expectations of stakeholders that may include the shareholders, board of directors, management, legislative bodies, public entities, regulatory bodies, and public interest groups.
- Allowances and/or restrictions contained in the internal audit charter.
- Disclosures required by the *Standards*.

- Audit coverage of the activities or responsibilities undertaken by the internal auditor.
- Significance of the operational function to the organization (in terms of revenue, expenses, reputation, and influence).
- Length or duration of the assignment and scope of responsibility.
- Adequacy of separation of duties.
- Whether there is any history or other evidence that the internal auditor's objectivity may be at risk.

If the internal audit charter contains specific restrictions or limiting language regarding the assignment of non-audit functions to the internal auditor, then disclosure and discussion with management of such restrictions is necessary. If management insists on such an assignment, then disclosure and discussion of this matter with the board is necessary. If the internal audit charter is silent on this matter, the guidance noted in the points below are to be considered. All the points noted below are subordinate to the language of the internal audit charter. When the internal audit activity accepts operational responsibilities and that operation is part of the internal audit plan, the CAE needs to:

- Minimize the impairment to objectivity by using a contracted, third-party entity or external auditors to complete audits of those areas reporting to the CAE.
- Confirm that individuals with operational responsibility for those areas reporting to the CAE do not participate in internal audits of the operation.
- Ensure that internal auditors conducting the assurance engagement of those areas reporting to the CAE are supervised by, and report the results of the assessment, to senior management and the board.
- Disclose the operational responsibilities of the internal auditor for the function, the significance of the operation to the organization (in terms of revenue, expenses, or other pertinent information), and the relationship of those who audited the function.

The auditor's operational responsibilities need to be disclosed in the related audit report of those areas reporting to the CAE and in the internal auditor's standard communication to the board. Results of the internal audit may also be discussed with management and/or other appropriate stakeholders. Impairment disclosure does not negate the requirement that assurance engagements for functions over which the CAE has responsibility need to be overseen by a party outside the internal audit activity.

6. Objectivity The CAE should continuously seek out ways to improve the level of objectivity throughout audit and some of the relevant matters have been mentioned earlier. A great deal of this hinges on installing suitable policies and procedures. The aim being to remove any potential barriers to the auditor's ability to perform fair and unbiased work. IIA Standard 1120 covers individual objectivity and says that:

> Internal auditors must have an impartial, unbiased attitude and avoid any conflict of interest.

While Practice Advisory 1120-1 provides some guidance on this topic:

- Individual objectivity means the internal auditors perform engagements in such a manner that they have an honest belief in their work product and that no significant quality compromises are made. Internal auditors are not to be placed in situations that could impair their ability to make objective professional judgements.

- Individual objectivity involves the CAE organizing staff assignments that prevent potential and actual conflict of interest and bias, periodically obtaining information from the internal audit staff concerning potential conflict of interest and bias, and, when practicable, rotating internal audit staff assignments periodically.
- Review of internal audit work results before the related engagement communications are released assists in providing reasonable assurance that the work was performed objectively.
- The internal auditor's objectivity is not adversely affected when the auditor recommends standards of control for systems or reviews procedures before they are implemented. The auditor's objectivity is considered to be impaired if the auditor designs, installs, drafts procedures for, or operates such systems.
- The occasional performance of non-audit work by the internal auditor, with full disclosure in the reporting process, would not necessarily impair objectivity. However, it would require careful consideration by management and the internal auditor to avoid adversely affecting the internal auditor's objectivity.

8. Planning work areas An audit department with no formal audit plans can never be said to be independent. Not only are professional audit standards being flouted but it also means that audit responds to the pressures of the day, normally on a 'he who shouts loudest' basis. This turns the audit resource into a political football that is used and abused on the excuse of providing a client responses-based audit service. A CAE who allows this disastrous condition to arise will be open to criticism.

Professionalism

This is based on employing qualified staff and ensuring they operate to professional standards. The principle of using unqualified staff who are able to operate on a similar level is inconsistent since there is then no reason why they should not have secured the full qualification. Since they are not members, they have no real allegiance to the methodologies that underpin professional audit services. Non-professionals will be employed where salary levels are relatively poor which means that the status of audit will likewise suffer as will the ensuing level of independence. Managing a tight audit budget and possibly competing against external suppliers of audit services may mean that audit staff should not be too expensive. Automated audit techniques will help as will a policy of employing a few junior staff for detailed checking. As long as supervisory auditors are qualified they should be able to work to quality standards.

Managing the Director of Finance

There are some internal audit units that are located within the DF's department. Politicians, when considering legislation on accountability, view the internal audit role as primarily concerned with promoting financial accountability on behalf of the chief financial officer. This is a fundamental misunderstanding of the true audit role as it fails to recognize that we cover systems at a corporate, managerial and operational level that includes the financial implications therein. It is nonetheless impossible to ignore forces (i.e. legislation) directed at expanding the audit role and profile. We will, however, have to address two basic questions when reporting to the DF:

- Can we be truly independent in auditing the financial systems?
- If we were in dispute with the DF on an audit related issue how would this be resolved?

Being in the pocket of the DF is an unfortunate situation that the CAE may experience as a result of the political forces of the day and the assumed reporting line. Where this arises one's only real option for retaining professional integrity may be to resign on principle. Having support from the board is important in balancing out the power relationships and extracts from Practice Advisory 1110-1 (Organizational Independency – for standard 1110) gives some practical advice. Standard 1110 states:

> The chief audit executive must report to a level within the organization that allows the internal audit activity to fulfill its responsibilities. The chief audit executive must confirm to the board, at least annually, the organizational independence of the internal audit activity.

While advisory 1110-1 goes on to suggest:

> Support from senior management and the board assists the internal audit activity in gaining the cooperation of engagement clients and performing their work free from interference.
>
> The chief audit executive (CAE), reporting functionally to the board and administratively to the organization's chief executive officer, facilitates organizational independence. At a minimum the CAE needs to report to an individual in the organization with sufficient authority to promote independence and to ensure broad audit coverage, adequate consideration of engagement communications, and appropriate action on engagement recommendations.
>
> Functional reporting to the board typically involves the board:
>
> - Approving the internal audit activity's overall charter.
> - Approving the internal audit risk assessment and related audit plan.
> - Receiving communications from the CAE on the results of the internal audit activities or other matters that the CAE determines are necessary, including private meetings with the CAE without management present, as well as annual confirmation of the internal audit activity's organizational independence.
> - Approving all decisions regarding the performance evaluation, appointment, or removal of the CAE.
> - Approving the annual compensation and salary adjustment of the CAE.
> - Making appropriate inquiries of management and the CAE to determine whether there is audit scope or budgetary limitations that impede the ability of the internal audit activity to execute its responsibilities.
>
> Administrative reporting is the reporting relationship within the organization's management structure that facilitates the day-to-day operations of the internal audit activity. Administrative reporting typically includes:
>
> - Budgeting and management accounting.
> - Human resource administration, including personnel evaluations and compensation.
> - Internal communications and information flows.
> - Administration of the internal audit activity's policies and procedures.

Reconciling the Consultancy Branch

The internal auditing arena is now facing a real threat to independence where it is being asked to reconcile two forces that are at times in conflict as in Figure 5.9. The client might wish to have internal audit perform a series of consultancy projects generated by ad hoc problems that they as managers may experience. The professional auditing standards seek to promote audits that involve

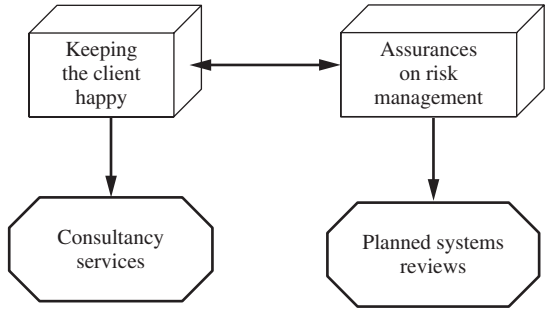


FIGURE 5.9 Consultancy versus systems work.

reviews of control systems as a service to the entire organization as a wider concept. The conflict arises where the problems referred to audit by management result from inadequacies in controls. The act of propping up management reinforces the view that management need not concern itself about controls and that if there are control faults, audit will solve the ensuing problems. Here independence falls by the wayside and a response-based audit service is resourced to the detriment of organizational controls. We will argue that the following holds true:

> Unqualified staff employed in an audit unit that is located in the finance department to provide a response-based service to managers will be unable to meet the requirements of professional auditing standards (including the requirements for independence).

There are a number of ways to reconcile the competing forces present where consultancy and audit services conflict:

- The audit charter should make clear that consultancy services are provided in addition to main-line audit services. Formal definitions will be required along with an explanation that makes clear the differences between these two types of services. Audit services would be based around planned systems reviews while consultancy consists of any other services that the client may require.
- These additional consultancy services should not mean that the audit plan is not completed. Consultancy services should be separately resourced so as not to detract resources away from the audit plan. The approved audit plan is in fact a contract with the organization and each project should be delivered in discharging the audit role. Consultancy services on the other hand consist of contracts with individual managers scattered throughout the organization.
- Where management referrals highlight the presence of control weaknesses in particular areas, the in-built flexibility of audit plans should allow these plans to be adjusted as a result of changing control priorities and risks. As such management problems are not simply ignored and if these relate to poor controls then audit plans should be adjusted so that high risk audits are featured. In this situation management's control concerns are not deemed to be consultancy work, but simply mean a change in planned audit priorities. It is only when management's problems do not relate to improving control that they fall under the category of additional client-based services.
- One way of emphasizing the distinction between audit and consultancy services is to ensure that they are provided by different audit groups. This solves many problems relating to role

definition and client contact. The difficulty is where the work becomes so far differentiated that they cannot really work together in teams. The other problem is that separate funding sources may mean that one side progresses more than the other. We have to mention the real possibility of professional jealousy where one type of work, say CRSA workshops (i.e. consultancy), is deemed more attractive than the other. These issues will have to be resolved by the CAE by careful consideration and insight.

- Where there is a conflict between consultancy and audit services, then audit services should reign supreme. This requirement should be formally stated in all agreements for the provision of consultancy services. As an example, say a consultancy project into poor performance finds a massive breach of important control arrangements, this may mean the operation will appear in the audit plans as a newly defined high risk area. We will have to provide consultancies with this in mind on a 'take it or leave it!' basis. Anything less than this is unacceptable and interferes with audit independence.
- Additional resources should be secured for major consultancy projects since, if they are deemed important, management will presumably be prepared to pay for them. A useful technique is to employ temporary staff to resource consultancy work and charge them directly to the client's budget. It is important that the project is costed at the outset so that these additional consultancy charges are agreed with the client. The work will obviously be led and directed by the in-house lead auditor.
- The CAE should also make clear that any breach of procedure uncovered in the project will be reported to the appropriate officers. Internal irregularity discovered during the audit must be dealt with as issues of probity and not 'glossed over' as is possible with management consultants who have no particular allegiance to the organization. Again where management fails to accept this concept they presumably will not wish to employ consultancy work from the internal audit function.

David M. Felten has warned of the dangers of the Spock-like internal auditor:

> Maintaining an adequate level of objectivity is a constant concern for internal auditors. Unfortunately, some auditors seem to feel that to be totally objective, one must exercise a 'Spock-like' personality when interacting with auditees. The focus point for these auditors becomes the audit finding, or, even worse, the need to produce an audit finding. There is a fear that empathizing with the needs and concerns of the auditee will somehow compromise the auditor's ability to be rational and logical in determining and analyzing a control weakness or deficiency and in recommending an appropriate correction.[13] Independence cannot be guarded at all costs and only sufficient independence is needed to enable professional audit work to be carried out and acted on by management. The auditor must balance the right to plan areas of work with the need to involve management in this process. Providing a response-based audit service with no formal audit plans will secure support from management but at the same time will diminish independence severely. The auditor cannot be a slave to independence, but at the same time a lack of it will undermine the entire audit role. As part of this process of balancing the various relevant factors, the need to adopt professional audit standards and well-thought-out policies and procedure becomes a fundamental prerequisite. We have developed four levels at which the issue of independence can be addressed by the CAE that cover the adopted structures, staffing, strategy and systems. For each of these four fundamental components it is possible to add further subcomponents to add to the detail. We can suggest that the degree to which these factors are in place equates to the degree of independence that has been secured, since the real purpose of internal audit is to help an organization perform through the provision of advice and reliable

(independent) assurances. The future of internal audit may mean that they will report formally to the audit committee which in turn will report to the shareholders. Building on this point, perhaps there might even be a direct reporting line from the internal auditor to the shareholders?

5.6 Audit Ethics

The auditing profession is charged with providing a high standard of audit services to each employing organization and the audit charter forms a contract with the organization in this respect. An extension of this concept is the view that audit professionals are also charged with performing their work with the highest of moral standards that one would expect from people in this position. Moreover the code of ethics (or code of conduct) forms a contract to cover the auditor's moral obligations. The organization may therefore rely on this code for guiding the conduct of members of the audit department. The IIA consider that the purpose of the IIA code of ethics is:

> To promote an ethical culture in the profession of internal auditing. A code of ethics is necessary and appropriate for the profession of internal auditing, founded as it is on the trust placed in its objective assurance about risk management, control and governance. The Institute's Code of Ethics extends beyond the Definition of Internal Auditing to include two essential components:
>
> 1. Principles that are relevant to the profession and practice of internal auditing; and
> 2. Rules of Conduct that describe behaviour norms expected of internal auditors. These rules are an aid to interpreting the Principles into practical applications and are intended to guide the ethical conduct of internal auditors.
>
> The Code of Ethics provides guidance to internal auditors serving others. 'Internal auditors' refers to Institute members and those who provide internal auditing services within the Definition of Internal Auditing.

Relevant Factors

The IIA Code of Ethics is reproduced below:

Principles

Internal auditors are expected to apply and uphold the following principles:

1. *Integrity*
   The integrity of internal auditors establishes trust and thus provides the basis for reliance on their judgment.
2. *Objectivity*
   Internal auditors exhibit the highest level of professional objectivity in gathering, evaluating, and communicating information about the activity or process being examined. Internal auditors make a balanced assessment of all the relevant circumstances and are not unduly influenced by their own interests or by others in forming judgments.

3. Confidentiality

Internal auditors respect the value and ownership of information they receive and do not disclose information without appropriate authority unless there is a legal or professional obligation to do so.

4. Competency

Internal auditors apply the knowledge, skills, and experience needed in the performance of internal audit services.

Rules of Conduct

1. Integrity

Internal auditors:

1.1 Shall perform their work with honesty, diligence, and responsibility.
1.2 Shall observe the law and make disclosures expected by the law and the profession.
1.3 Shall not knowingly be a party to any illegal activity, or engage in acts that are discreditable to the profession of internal auditing or to the organization.
1.4 Shall respect and contribute to the legitimate and ethical objectives of the organization.

2. Objectivity

Internal auditors:

2.1. Shall not participate in any activity or relationship that may impair or be presumed to impair their unbiased assessment. This participation includes those activities or relationships that may be in conflict with the interests of the organization.
2.2. Shall not accept anything that may impair or be presumed to impair their professional judgment.
2.3. Shall disclose all material facts known to them that, if not disclosed, may distort the reporting of activities under review.

3. Confidentiality

Internal auditors:

3.1. Shall be prudent in the use and protection of information acquired in the course of their duties.
3.2. Shall not use information for any personal gain or in any manner that would be contrary to the law or detrimental to the legitimate and ethical objectives of the organization.

4. Competency

Internal auditors:

4.1. Shall engage only in those services for which they have the necessary knowledge, skills, and experience.
4.2. Shall perform internal audit services in accordance with the International Standards for the Professional Practice of Internal Auditing.
4.3. Shall continually improve their proficiency and the effectiveness and quality of their services.

Introduction The purpose of The Institute's Code of Ethics is to promote an ethical culture in the profession of internal auditing.

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.

A code of ethics is necessary and appropriate for the profession of internal auditing, founded as it is on the trust placed in its objective assurance about risk management, control and governance. The Institute's Code of Ethics extends beyond the definition of internal auditing to include two essential components:

1. Principles that are relevant to the profession and practice of internal auditing;
2. Rules of conduct that describe behaviour norms expected of internal auditors. These rules are an aid to interpreting the Principles into practical applications and are intended to guide the ethical conduct of internal auditors.

The Code of Ethics together with rest of the Institute's IPPF and other relevant Institute pronouncements provide guidance to internal auditors serving others. 'Internal auditors' refers to Institute members, recipients of or candidates for IIA professional certifications, and those who provide internal auditing services within the definition of internal auditing.

Applicability and Enforcement

This Code of Ethics applies to both individuals and entities that provide internal auditing services. For Institute members and recipients of or candidates for IIA professional certifications breaches of The Code of Ethics will be evaluated and administered according to the Institute's Bylaws and Administrative Guidelines. The fact that a particular conduct is not mentioned in the Rules of Conduct does not prevent it from being unacceptable or discreditable, and therefore, the member, certification holder, or candidate can be liable for disciplinary action.

There is an expectation from each and every internal auditor that they should:

Be honest and diligent Here honesty is seen as essential and this sets the tone for the rest of the code. Objectivity is part of the process of achieving independence and again is a fundamental component of auditing. Diligence is less exciting an ideal but is as equally important as the rest in that it needs a dogged determination to achieve clear goals by basic hard work. This lifts audit from the spiritual level to a work-based function that requires a degree of dedication. To be truthful, fair and hardworking is all that can be asked of an employee. The main problem here is that it is difficult to measure these concepts as they tend to be embodied within one's personality. It would take a degree of legal reasoning to establish if someone has breached any of these pointers, and it is not something that can be readily measured on a day-to-day basis. One may spot a severe case of a dishonest auditor but it is less easy to measure degrees of, say, honesty on the basis that one auditor is more honest than another. Nonetheless these are important components and do have a clear meaning to the everyday person in the street.

Not get involved in illegal activity This provision brings in the external environment and one interpretation is that members convicted of criminal offences, the nature of which reflects badly on the auditing profession may find themselves excluded from membership. Any infringement of this princple should result in the member being before the IIA for deliberation and decision with all members being treated similarly. The key point is that ethics enters into the private life of the practising auditor and attaches to his/her behaviour even outside the work environment.

Contribute to the ethical objectives of the organization This reconciles two potentially conflicting principles. There is above all an affiliation to the employer which for all practical purposes makes good sense. On the other hand there is a caveat whereby the auditor cannot become involved in illegal matters. This is somewhat incomplete in that the auditor will generally not be involved (i.e. party to) improper acts but will be aware of them as part of the audit office. To sit back and not comment on possible probity problems or to be refused access to sensitive areas where probity has not been achieved, can be explained as part of this process of being loyal to the organization. Admittedly it is rare for an entire organization to be corrupt, although, as the BCCI case shows, it is not impossible. What is more likely is for top managers not to care what their staff do so long as certain goals (e.g. defined profit margins) are being achieved. The difficulty arises where the two parts of this element of the code of ethics are mutually exclusive. Here the auditor's resignation would appear to be most appropriate, although this is not always possible particularly where the economy is in recession.

Preserve an unbiased assessment *This covers those activities or relationships that may be in conflict with the interests of the organization*. Here one would consider any activities that may not be acceptable where the internal auditor is employed by the organization. As an example, visualize an auditor who engages in a business relationship with a main client for audit services that impairs his/her ability to carry out good audit work. The first part of this item is in itself quite interesting; the rule may be seen as part of a wider requirement to promote the interests of the organization. It imposes on the auditor a high level of commitment to the organization that may not attach to other employees. As such it does make the IIA code somewhat demanding, which cannot be a bad thing for the profession.

Conflict of interest is defined by the IIA as:

> Any relationship that is, or appears to be, not in the best interest of the organization. A conflict of interest would prejudice an individual's ability to perform his or her duties and responsibilities objectively.

Not accept gifts that would impair professional judgement The main implications of this factor are that gifts and bribes are more or less banned. A useful addition is the concept of presumption that gifts impair judgement. In practice there is no defence against such an accusation. One need only prove that an outsider would assume a relationship between receiving gifts and giving an audit opinion, rather than show an actual cause and effect. The only real problem is related to materiality since value may be defined as anything of any worth. Alternatively it may be seen as a real-life concept that sees value as something that is great enough to influence behaviour. The final point to note is the notorious difficulty in discovering a bribe that has been well organized. Notwithstanding this, if auditors abide by this part of the code of ethics then all uncertainty is removed. Impairments is defined by the IIA as:

> Impairment to organizational independence and individual objectivity may include personal conflict of interest, scope limitations, restrictions on access to records, personnel, and properties, and resource limitations (funding).

Not disclose confidential material This rule provides a significant source of protection for the rights of the auditor and may be seen as the true ethical standard that lifts audit work to a higher plane. It can be summed up in the age-old adage 'report and be damned', which makes internal audit quite different from other management services who are bound by their client. If

we were to operate without this provision, there would be very little of the ethical considerations that make the audit task at times somewhat difficult. As it stands the auditor cannot simply pursue the task of satisfying management. The findings become the paramount factor in the audit report and these must be fully reported. The requirement to report may result in a dilemma when all those officers surrounding the auditor either do not wish this report to be made, or intend to take no notice of it. In one sense the auditor is only required to report and cannot force managers to act since publishing the report discharges the main audit obligation. Herein lies the main reason why 'whistle-blowing' is now a fundamental issue to many internal auditors. The complete ban from disclosing information that has not been authorized for use by third parties can be read into this part of the code. One might argue that the welfare of the organization relates only to legal objectives that may be pursued by those who run and direct the business. However, there is a problem where the entire organization is corrupt. Here the auditor may well consider that the code of ethics acts as a restriction in alerting the authorities and getting 'the organization' into trouble. We can go on to suggest that the only acceptable reason why a CAE may wish to suppress the findings of a member of audit staff would be that it is against the interests of the organization. Again the code of ethics binds the auditor to confidentiality and makes it difficult to take any action that falls outside what is allowed by line management. The basic principle of keeping information private is sound, but we can go further and propose that the auditor is duty bound to refrain from engaging in gossip, rumour and social discussion where matters that have come to his/her attention as a result of an audit are disclosed, even where there is no actual gain.

Be competent There is a clear link between this rule and the laws of negligence in that staff are required to turn down work that they cannot perform or at least to seek assistance. We might, however, expect some role for audit management as they are responsible for setting work and ensuring that it is done to professional standards. One would not expect an individual member of internal audit to question an assignment that has been given to them by an audit manager. This may not go down too well. Likewise it would be embarrassing for a junior auditor to point out that this requirement of the code of ethics may be infringed. It is probably better to build the competence factor into the audit manual and force audit staff to bring to their manager's attention any reason why an assignment cannot be properly completed. At the same time the CAE should be required to examine this factor whenever work is assigned and then undertaken. It becomes an organizational issue rather than a matter for individual auditors. This makes it more appropriate for it to be dealt with via the auditing standards as opposed to (or as well as) the code of ethics.

Compliant with standards This catch-all category simply reinforces the point that the onus is on the auditor to comply with the requirements of the code of ethics and goals of the IIA. This may be seen as the most far-reaching part of the code as it brings into play the entire package of professional auditing standards. What it might have gone on to say is:

> The IIA will seek to review compliance with this and the other provisions of the code and will bring disciplinary action against any member who fails to comply with it.

Seek continuous improvement The true professional has an affiliation with the service that is being delivered as a conceptual issue over and above the day-to-day work that is carried out. This internalized desire to seek improvements distinguishes the proficient auditor from the clerical record checker as a higher plane is sought. It must revolve around a strategic plan that sets direction and standards for the audit service which should be the key responsibility of the CAE.

Each internal audit department is advised to establish a suitable code based on the above but tailored to meet its specific requirements and organizational policies. Adherence to this code should be contained in the auditor's job description and the code should be fully set out in the audit manual.

Underlying Models

The late Gerald Vinten has developed three models of morality:

The regulatory model This approach sees the question of morals being based on instructions from the appropriate authorities. As such one is told what to do and rewarded for following instructions. Regulation is also based on the threat of punishment where the rules are breached. Rules must be applied with care as they can backfire if this is not the case:

> An employee's wife dies after an extended illness, and colleagues circulate an envelope around the office to collect donations for flowers. A supervisor abruptly stops the process, however, noting that company policy strictly prohibits any solicitation of employees on company premises. Far-fetched? Perhaps, but this incident actually happened in a company where a new set of policies had been issued. When compliance initiatives focus too narrowly on rule-following and the threat of sanctions – even at the expense of common sense – genuine and effective compliance is likely to be lost. Instead, organizations should build a shared commitment between management and employees in doing the right thing – a commitment that is based on an understanding of the 'why' behind the rules. A commitment environment includes – but moves beyond – compliance. It supports compliance and controls but also precipitates responsible behaviors that yield positive results.[14]

The aspirational model This model appeals to the higher levels of humanity with the concept of morals seen as something that glows from within. The feeling that people are born with a sense of morality pervades this model although there are problems where the aspirations are not being met.

The educational model This is the most appropriate model where morality is seen as a set of concepts that may be learned. The professional approach is linked into the demanding training and development programme that is followed by members of the internal auditing profession. This model has a great deal of scope and allows for the different views that people have on the topic of moral behaviour.

The above models can be used to build suitable frameworks for personal conduct. Even so, we return to the vexed question facing internal auditing where there would appear to be no duty owed to society at large outside of the requirement for loyalty to the employer. Some argue that the internal auditor can go further and help design the corporate code of ethics:

> Internal auditors should participate in the development of a company code of conduct, and reviews of the code should be performed on a regular basis by reviewing the literature and evaluating feedback from various segments within the company. Audits that measure employee understanding and adherence with the codes should be designed. Since many organizations change rapidly, procedures for incorporating emerging issues may need to be built into the code, thereby maintaining it as a living document.[15]

Whistle-blowing

This is where the internal auditor releases confidential information to an outside authority knowing that the senior management in the organization would have forbidden it. This might occur where the auditor has uncovered a breach of regulation or legislation and finds that management wishes to suppress it. An example would be falsification of testing data by a cosmetics company to satisfy the regulatory authorities before releasing a new product onto the market. The auditor then decides to disclose the details to the appropriate authorities on the basis that it is a professional duty to society. Where this occurs the auditor tends to suffer. Dismissal, unemployment and a tarnished reputation are likely to follow. Unfortunately, there was little protection available to support the auditor. There is conflict between auditors' duty to society and professional loyalty and confidentiality to the employer. The Public Interest Disclosure Act 1998 applies to England, Scotland and Wales and covers disclosures relating to crimes, breaches of legal obligations, miscarriage of justice, dangers to health and safety or the environment and concealing information relating to these items. Protected disclosure relates to criteria that include:

- reasonable belief that elements above (crime, etc.) are involved;
- made in good faith;
- not for personal gain;
- internal processes already fully utilized.

The burden of proof for the above rests with the employee and internal procedures can only be avoided where:

- employee believes s/he would be 'subject to a detriment' if disclosure made to the employer.
- evidence would be concealed by employer.
- employee has already made a disclosure of substantially the same information.

If internal procedures are unsafe then any official regulator should be informed (i.e. the prescribed body). For public sector employees, information classified, say, under the Official Secrets Act does not benefit from the Public Interest Disclosure Act's protection. Gagging clauses are probably void under the Act. Employees dismissed as a result of protected disclosure should make representation to the employment tribunal within seven days of the dismissal. Before this legislation came onto the statute books, the IIA had issued a proclamation that suggests that a number of tests should be applied to any one potential whistleblowing situation:

1. Is the audit department complying with IIA standards?
2. Does the CAE have direct access to an audit committee where the facts have been fully reported?

If these two requirements are met, then there is generally no need to report outside the organization. If they are not, then the problem is compounded and legal advice should be sought. The clear allegiance to the employer is seen in the IIA statements. An old IIA Briefing Note number Five (1994) dealt with the 'vexed issue of whistleblowing' by focusing on the professional issues involved. The IIA have developed a definition of whistleblowing:

> The unauthorized disclosure by internal auditors of audit results, findings, opinions, or information acquired in the course of performing their duties and relating to questionable practices.

One key point that is made by the briefing note is that the existence of an audit committee falls in line with best professional practice. This committee is most effective where it agrees the appointment and removal of the CAE. This factor in conjunction with adequate reporting lines promotes the ability to achieve the IIA's professional auditing standards. The briefing note suggests that the CAE has a duty to report audit findings and if these are not sufficiently addressed then reports should be sent to higher levels within the organization. The lack of a properly constituted audit committee would make it difficult to apply this principle. Disclosure to external parties should either be authorized by the organization or fall under a legal obligation to do so (e.g. under a court order). The role of internal audit as an advisory function with no executive responsibility for correcting systems faults is reinforced. The correction of wrongdoings is seen as falling outside the jurisdiction of the auditor since once problems have been reported, it is up to management (e.g. the board of directors) to take appropriate action. The more junior auditor who feels that audit management has not adequately addressed a finding is also bound by the rules on official reporting lines. Where audit seeks to report these matters to external interested parties, this is seen as destroying the relationship between management and their internal auditors (but note the Public Interest Disclosure Act). The briefing note goes on to summarize the position where auditors are able to use authorized reporting lines. Once exhausted, there is no further remit to report elsewhere even if the auditor has since resigned. The realities of whistleblowing are hinted at when the briefing note argues that:

> An auditor should weigh these considerations with great care. He or she should be aware that whistleblowers who 'go public' have found it extremely difficult to enter similar employment elsewhere.

IIA standard 2420 on the quality of communications makes it clear that all relevant information should be reported by the internal auditor:

> Communications must be accurate, objective, clear, concise, constructive, complete, and timely.

Interpretation:

Accurate communications are free from errors and distortions and are faithful to the underlying facts. Objective communications are fair, impartial, and unbiased and are the result of a fair-minded and balanced assessment of all relevant facts and circumstances. Clear communications are easily understood and logical, avoiding unnecessary technical language and providing all significant and relevant information. Concise communications are to the point and avoid unnecessary elaboration, superfluous detail, redundancy, and wordiness. Constructive communications are helpful to the engagement client and the organization and lead to improvements where needed. Complete communications lack nothing that is essential to the target audience and include all significant and relevant information and observations to support recommendations and conclusions. Timely communications are opportune and expedient, depending on the significance of the issue, allowing management to take appropriate corrective action.

Applying a Three-Part Model

It is possible to adopt a model of ethical considerations that helps direct the conduct of the auditor in Figure 5.10.

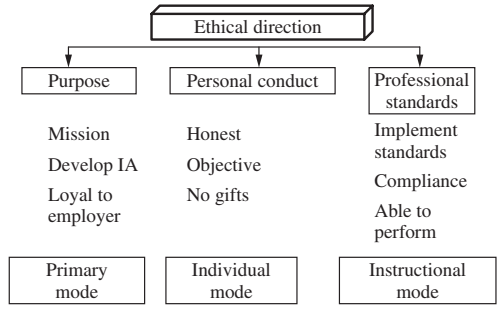


FIGURE 5.10 A model of ethical considerations.

Some explanations follow:

1. The **purpose** forms the goals of the auditor as a form of conceptual guide that sets an overall direction of the audit effort. It is considered a primary code in that it provides this fundamental standard that determines the mission of the auditor, the need to develop the profession and an essential loyalty to the employer.
2. The **personal conduct** attaches to the daily activities of the individual auditor in its requirement for basic honesty and objectivity. This calls for high standards over the way individuals conduct their private and working lives, which, for example, makes it hard for a convicted criminal to perform an audit role.
3. **Professional standards** are linked more to the instructional component of the auditor's development. Here we are concerned with the way auditing standards are used and complied with by qualified persons.

We can now build on this model and look for key additional components of the ethical framework that would promote three basic matters:

- Honest and sincere auditors who have an honest desire to objectively conduct good audit work and prepare fully their findings.
- An audit function that is able to report all findings in a full and open manner notwithstanding the pressures to 'play the organizational game'.
- An organization whose corporate body expects the highest ethical standards from all employees and top management, and supports any audit report that impacts on this issue.

The code of ethics is in fact a series of codes each of which depends on the individual auditor, the audit unit and the entire organization. If there are gaps in any of these three parts, then a suboptimal position arises. The code of ethics creates a special bond between the auditor and the employer. The internal auditor's position is easily abused and there are not many officers who will question the auditor's behaviour particularly where it appears that audit reports to some unseen higher authority. The code counters this problem and should be applied in an educational mode where auditors are encouraged to adopt the code as part of the training and development process.

5.7 Police Officer versus Consultant

Most audit textbooks make reference to the impact that internal audit has not only on systems but also on people, and stress the importance of understanding human behaviour. This is sometimes

extended by the view that auditors face various complicated issues because of their special position in the organization. The alternatives to the word 'Audit' from a standard thesaurus include the following terms:

examination	*review*
investigation	*inspection*
scrutiny	

These terms do not conjure up the concept of a helpful, value-added service and here we tackle the fall-out of negativity and the need to manage this problem by adopting the stance that merely being genuine is not enough. One has to seriously consider one's position and the impact of the applied audit policies on the behavioural aspects of this role, to uncover any actual or potential barriers to good performance. Alan Marshall outlines his approach when asked by someone 'So what do you do for a living?': 'The word "audit" has negative connotations, fostering the image of tick and turn . . . When announcing that I work as internal auditor . . . perhaps the most frustrating reaction is "Ah! You're an accountant. You check people's books, don't you?"[16]

Human Behavioural Aspects

This covers a wide area and touches on topics such as industrial psychology, communication skills and group theory. Auditors should be skilled in dealing with people and as such this aspect is seen as a valid audit skill. Unfortunately this skill does not always form part of the auditors' professional training and development programme. In fact a poor recruitment policy may result in bringing in auditors who see little value in developing good inter-personal skills. The old-fashioned detailed checker had little time to discuss the real-life issues that fall outside the scope of the audit programme. Nowadays auditors are required to do more than operate on a detailed technical level; they are expected to be able to converse openly with senior management. Dale Flesher has written about this principle:

> The auditor's effectiveness in developing a good relationship with the employees of the audit client is probably the key to success. The traits most needed include confidence, objectivity, persuasiveness, and personal magnetism. The confidence in one's ability and judgment and the courage to stand firm are essential to an internal auditor.[17]

1. Mautz and Sharif[18] These authors feel that internal control is essentially about people, which again highlights the need to frame audit work with this concept in mind. A large part of the control system depends on a close interface with the people who are involved in the system. An ability to understand documentation and system manuals comes a poor second to the need to appreciate how managers, supervisors and staff interact with the system so as to promote an acceptable degree of control. In contrast, if these people are simply ignored, it is doubtful whether one would be able to assess the relevant controls and form a sensible opinion.

2. The one-minute manager Research into the 'one-minute manager' shows that formal long-winded audit reports have little impact on busy managers. They want to know in short simple words 'what the problem is, and what they should therefore do about it'. While the auditor may present with pride a 50-page report containing ten separate appendices, it is doubtful whether this will be fully read by anyone, no matter how well written. Understanding the managers' needs and how the audit role may fit into this will help circumvent the frustrating process of producing audit reports that have little or no real use to managers (and the organization).

3. Audit intrusion However well meaning the auditor is, his/her intrusion into a manager's work area may well contribute to an increase in the overall level of managerial stress. The well-meaning opening phrase, 'Can I help you?', which the auditor, may use to introduce his/her audit, may be met with a cold silence with unspoken undertones of, 'Yes, by going away and letting me get on with my job!' If we were management consultants we might then withdraw from the audit, but since this is not the case there is no simple answer.

4. Relevance An audit approach that is obsessed with listing minor errors that occurred months ago, while at the same time ignoring issues affecting the whole future of the operation being reviewed, will have very little relevance to management. Auditors trapped in this obsession with basic detail are doomed to become obsolete with the passing of time, while professional auditors offer unlimited horizons. The old attributes of reliability and total accuracy (to the *n*th degree) are being replaced by newer ones of creativity and genuine enthusiasm linked into a commitment to organizational goals. A paper by CIPFA dealt with the perception of audit quality:

> Some 71% of chief financial officers said they thought internal audit has an 'image problem,' and there was a 'quality expectations gap' in relation to internal auditing . . . There are two major obstacles to improving the image of internal auditing:
>
> - internal auditing do not understand the perceptions of their customers; and
> - customers do not understand the modern role and objectives of internal audit.
>
> To survive and prosper, internal audit will have need to target its key customers, bridge the expectations gap and establish itself at the heart of the organization as a facilitator of change and a marketer of imaginative solutions.[19]

5. Management controls Internal auditors who fail to recognize that the most fundamental control is the management process itself will necessarily perform substandard work. The ability to step into the management process is a major achievement.

6. Management needs Internal auditors who fail to appreciate management's needs will be unable to formulate sensible recommendations and as a result will leave themselves open to competition from other review agencies. Unfortunately the success criteria that management is working within may not be wholly clear when the audit is first started. Firm inter-personal skills are required to establish just what management is trying to achieve which, bearing in mind the importance of this factor, will have a major impact on the resultant audit. Again, these skills are over and above the basic audit techniques that most auditors will study as part of their training programme.

As a response to the above issues, auditors have the difficult task of balancing the need to understand management with the equally important need to fulfil their professional obligation not to subordinate their judgement on audit matters to that of others. Nothing short of a truly professional approach, having due regard to the available research into behavioural aspects, will enable internal audit to achieve the desired results.

The Churchill Studies

This limited research carried out many years ago by Neil Churchill[20] was based on a pilot study of seven firms looking at auditees' attitudes towards internal audit. Attitudes towards internal audit were found to be as given in Table 5.1.

TABLE 5.1 Churchill–attitudes towards internal audit.

Attitude	%
Negative	26
Neutral	48
Positive	24
Mixed	2

TABLE 5.2 Whom auditor most resembles.

Resembles	%
Teacher	11
Policeman	58
Attorney	23
Mixed	8

When asked who internal auditors were most like the replies were broken down as shown in Table 5.2.

The results have to be treated with caution since they are based on limited research. There are also vague areas such as the idea of an attorney, who could be a defendant's best friend or alternatively could be perceived as prosecuting a helpless individual. The work made it clear, however, that feelings of suspicion, resentment and distrust of the internal auditor were felt by auditees.

IIA Survey – Mints

In 1972 the IIA.Inc. commissioned Frederick Mints to look into the auditee/auditor relationship and see what could be done about causes of unsatisfactory relationships.[21] The approach was to:

1. Analyse background material.
2. Look into available research.
3. Interview audit managers.
4. Carry out laboratory experiments where puzzles were solved in two environments, one with a positive team-based observer and the other with a critical formal observer giving the same advice. The observers were meant to represent the two different audit styles of advisor and inspector.
5. Carry out field study experiments applying the different styles using working conditions.

Mints highlighted views of internal audit behaviour. The police officer role saw good working relations as useful but not essential since, as long as the auditor was polite, this was enough. The consultancy approach was geared more to getting inside the managerial perspective based on positive working relationships. The main findings were:

1. Most audit managers felt that auditee relationships could be improved.
2. The participative style secured more favourable comments than the traditional style.
3. Audit managers' choice of style was as given in Table 5.3.

TABLE 5.3 Mints–choice of audit styles.

Traditional style (A)	*Mixed style (B)*	*Participative style (C)*
A	B B/C	C
8%	53% 11%	28%

Mints set out a number of ways that auditor/auditee relations might be improved:

1. better understanding and communications by the auditor;
2. use a mutual problem-solving rather than blame assignment approach in line with participative team building;
3. educate auditees in the usefulness of audits;
4. obtain management's view of the problem.

Other Research

Wood and Wilson Research in the 1990s by Wood and Wilson into behavioural aspects has, among other matters, identified a whole range of views from management concerning their opinion of the audit function. A long list of positive terms was invoked by management when discussing the auditors such as:

> helper, advisor, friend, expert

While others were not so complimentary, using terms along the lines of:

> inspector, police, informer, checker, gestapo

It would appear that feelings run strongly at both extremes and the auditor should bear in mind the various possibilities and where he/she might stand in the organization.

Audit Relationships

Internal audit cannot be done in the audit office with no contact with management and operatives. The audit objective is based on providing sound advice to management on their systems of risk and control. Here, the auditor requires a good understanding of the client's systems as a necessary prerequisite to effective audit work. It has been argued that internal control is really about people and if the people factor is missed then little useful work will ensue. The truly effective auditor is one who is able to extract all the required information from whatever source in an efficient manner. This requires talking to people, asking questions and securing assistance throughout the audit process and human relation skills may here be skilfully applied.

1. Internal audit liaison Contacts the auditor interacts with may include:

Audit management	Corporate managers
Operational managers	Operatives
Delegates at audit conferences	Government officials
Officials and lawyers	Finance and computer specialists
External auditors	Staff from other internal review agencies
Members of the public and customers	The organization's clients
Local police and the fraud squad	Auditors from other organizations

Each of these groups may require a different mode of communication and the auditors have to be flexible in meeting their expectations and at the same time satisfying the audit objective.

2. Transaction analysis Here relationships are formed with staff who may be of a junior or senior grade or be part of an individual's peer group. The relationships consist of various transactions as shown in Figure 5.11.

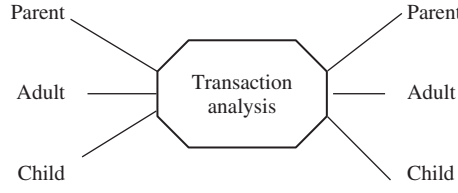


FIGURE 5.11 Levels of relationships.

The most efficient working model is where the 'adult' communicates with the 'adult'.

Emotional States (Role Playing)

Different people treat work in different ways and a major flaw in the human relations school of management theory is where employees do not see the work experience as a central life interest. It is possible to classify the emotional state of the employee under:

Withdrawal Where the employee feels unable to relate to work goals and so refuses to be committed to them. This can occur when the person feels frustrated by having their own views repressed by management. The result is that they minimize positive communications and become withdrawn.

Ritualistic Here the member of staff engages in an assortment of rituals that serve to confirm their position within the organization. It may be that they are referred to by their surname or have a larger desk or office because of their grade or length of service. This is symbolized by having 'the keys to the executive bathroom'. The model of company car offered will tend to be related to seniority.

Pastimes This person sees work as an interesting pastime and may spend much time gossiping, securing favours and generally enjoying the social side of work. An auditor operating in this mode will typically work on never-ending fraud investigations following the audit nose and tracking down

the perpetrators in a style reminiscent of that used in detective stories. Low productivity, long lunches and an extensive network of work friends and contacts are normally a feature of this approach.

Games Where the work culture is geared to excessive competition then a games culture may become the norm. This views success as dependent on another colleague's failure. Employees spend time catching each other out, gaining the upper hand and generally getting into favour with the power figures within the organization. Many major decisions are made with the aim of scoring goals against colleagues. An individual's own goals may at times coincide with organizational objectives but they may also serve to suboptimize performance. Overreliance on one main performance indicator, e.g. ratio of recoverable to non-recoverable audit hours worked, may lead to managers distorting results and so playing games.

Work activity This emotional state may best serve the organization in that it occurs where the individual is geared into work goals and has a clear well-defined purpose that he/she relates to. They are not easily side-tracked from these goals and the social aspects of working for an organization assume second place to getting the job done in an efficient manner.

Dealing with People

There are certain obstacles that the internal auditor may come across when carrying out audit work, many of which relate to the behavioural aspects of work:

1. Traditional tick and check Many auditors are seen as checkers who spend their time ticking thousands of documents and records. In this way management may treat the auditor as someone who has an extremely limited role that requires little skill and professionalism. At the extreme, managers may view audit staff with disdain and greet their presence with what can only be termed ridicule. This position can account for the strained atmosphere that many an auditor has faced when meeting with client managers at the outset of an audit. The perception that operational management is very busy doing important work while the auditor is simply checking some of the basic accounting data that relates to the area can create a great imbalance. This sets the auditor at a disadvantage from day one of the audit. Where the auditor is only concerned with detailed testing programmes then this view is actually reinforced (see Figure 5.12).

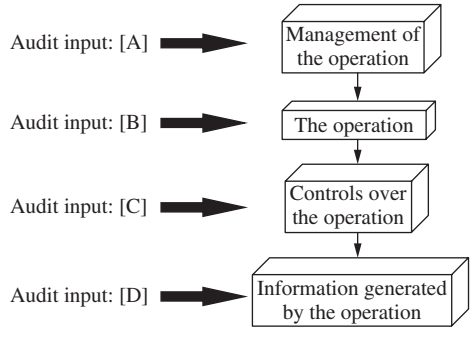


FIGURE 5.12 The implications of traditional tick and check.

The auditor may aim to work at level [C], i.e. deal with controls over the operation and ensure that these are adequate and adhered to. Work geared towards the operation itself [B] will take the auditor to a higher level since an understanding of the operational processes provides the foundation for a better audit. The management techniques [A] applied by senior officers act as the ultimate control in any system. Work at this level will pay great dividends. [D] represents the lowest level of audit work and if this approach is adopted, then, in contrast, it will reinforce the low esteem in which the auditor is held by management. Ticking and checking cannot justify the auditor's claim to professionalism.

2. The audit snoop Line management and the various operatives may resent the audit as being mainly based on management's wishes to spy on them using audit staff for this unsavoury task. It is management's job to establish suitable controls over the areas that they are responsible for. This includes installing information systems that provide feedback on the way staff are performing so that corrective action may be taken whenever necessary. It is not acceptable for managers simply to ignore this responsibility and rely on the annual internal audit to obtain information on what their staff are doing. This is an incorrect interpretation of both management's and audit's roles. The result is an arrangement whereby auditors are rightly seen as spies. Falling into this trap damages the audit reputation which, if continued, may become irretrievable. Where internal audit has not adopted this ill-conceived stance, then reliance may be given to staff at all levels in the area under review that audits are not acting as moles. The response in this case is to explain that audit reviews controls, not people; where people act as a control it is their role and not their behaviour that is being considered. This technique cannot be applied where we do in fact act as undercover agents for management.

3. Role of audit There are audits that are undertaken and completed with a final report issued some time after the event that have little meaning to the operatives affected by the work. Many see internal audit as part of the internal control that is centred on extensive testing routines. Where the auditor cannot explain the precise audit objectives it may be seen more as a punishment than a constructive exercise to assist management. This creates a mystique surrounding the audit role that may be fostered by an uncommunicative internal auditor.

4. Interviewing An audit interview may be a highly pressurized event for a more junior member of staff and if the auditor fails to recognize this, many barriers to communications may arise. The attitude of the auditor may be a crucial factor in determining whether the interview is successful or not. Audit objectives must be met but at the same time if the client's expectations are not satisfied (say in terms of clear explanations of the audit process) then the interviewee will be dissatisfied.

5. Audit committee The relationship with the audit committee is a factor in the success of the audit function. The committee constitutes a principal audit client, although the real support for audit comes from middle management who run the systems on a day-to-day basis. Bearing this in mind, the CAE will need to apply all his/her communications skills in forming a professional platform for the audit role.

6. Poor cousin of external audit Where the internal auditors merely support the external audit function, the relationship may leave little scope for professional development. Any prospective CAE should establish the precise position before accepting a new appointment and ensure that the organization is prepared to accept their interpretation of the auditors' terms of reference and scope of work.

7. Fear and hostility Auditors who feel that hostile management has something to hide will perpetuate a cycle of where they probe, and management resists, they probe harder and so on. Fear and hostility may result from managers being unsure of the audit role and how it should be geared into their objectives and needs and it is here that the auditor may in fact have caused the poor relationships.

8. Advisor/inspector conflict Problems will ensue where auditors are convinced that they are advisors whereas they are seen by management as only checkers. This results from a mismatch between words and deeds, where assurances are given to staff while at the same time searching for any errors that may be spotted, no matter how unimportant. The resulting audit report will not be influential if this reflects an obsession with error seeking.

9. Image problems Internal audit departments can have a poor reputation. This will affect the type of contact that they have with other members of the organization since one has to earn rather than demand respect. This can only be overcome if we adopt and apply professional standards and then seek to publicize this new-found image. There is some misunderstanding of the audit role and a need to improve overall image. Barriers to effective communications and problems when dealing with members of the organization may result. An attempt was made some years ago to change the name of internal audit to reflect the growing professional base that is now developing, although a suitable alternative was not forthcoming.

Understanding and Participating with Management

Where an auditor understands management and the management process it is easier to work in a partnership mode. The participative approach brings audit closer to a consultancy role where management needs are foremost. Many audit departments have moved along this route and the explanatory models suggest that a continuum may be designed where one may move further along the direction of participation. It must, however, be noted that the more participation that is promoted, the greater the strain in maintaining a satisfactory level of independence. As such there will be limits on how far one might go. It is possible to use an established model of audit styles ranging from a traditional through to a participative style. There is a continuum for each of the components of this established model as shown in Table 5.4.

TABLE 5.4 Traditional versus participative styles.

Factor	*Traditional style*	*Participative style*
Role	Policeman	Advisor
Authority	Formal	Informal
Source of authority	Office	Personal attributes
Sanction	Coercion	Suggestion

These are two extremes which might on the one hand mean that an audit function is imposed on management to police the organization. Alternatively, the audit service may be more like a partnership with audit providing professional advice in line with management's needs. Clearly modern internal auditing is moving towards the partnership role with management as it does not report to itself, or work towards its own mysterious goals.

1. Accounting staff Accounting staff are more used to working with formal controls and auditors, whereas operational staff may feel that the audit process is more of an intrusion. We are suggesting that internal audit will move far outside the limited world of financial systems and tackle any and everything that is important to the organization. While this sounds simple in theory, it does create many knock-on implications in terms of the effect this might have. Non-financial staff and managers may well find this uncomfortable, particularly where their only experience of an audit presence outside the finance department is where a fraud or breach of procedure is being investigated. This issue will need to be confronted and bridges built before any effective work may be carried out.

2. Basic planning Basic planning is a fundamental part of control and crisis management tends to be much more difficult to control in a systematic fashion. Before ascertaining what management does in terms of achieving its business objectives, it is well to go one step back and ask what it plans to do. The planning task provides a framework against which the actual results may be measured and it is here that the role of planning as a major control comes to the fore. Managers who are consistently deep in crisis tend to make great demands on audit services as problems mount up. The provision of these consultancy-type projects makes it more difficult to subsequently review the systems particularly where there are major weaknesses. In this scenario, trying to meet management's needs does not sit well with the task of reviewing the management process.

3. Budgetary control Budgetary control is an important management control which also has human behavioural implications. This is because success tends to raise performance while failure has a tendency to breed further failures. Again the 'people angle' of any control must be fully appreciated since it is little use recommending tighter budgets if this in fact demotivates staff and so impairs performance. As with all controls, it has to be implemented in a reasonable fashion having due regard to all the relevant factors, some quantifiable and others not so readily apparent.

4. Management style An auditor may find that management is applying a participative style where staff are treated as mature adults who want to perform. Alternatively, the style may be more akin to an authoritative approach involving management by fear. Besides affecting the overall performance this factor will also impact on the type of control systems in place in terms of fitting the defined culture. It is important that this factor is catered for during the audit process since it cannot simply be ignored. This can be difficult as culture is less tangible a product since it attaches to a whole body of people as opposed to one individual. It is still a significant component of the overall system of control and must be seen as such by the auditor.

5. Advantages of participation The auditor should recognize the culture that exists in the area being audited and ensure that audit recommendations are framed in a way that fits into management's needs. Participative auditing means working with management rather than auditing them. This is in line with the view that controls belong to management and they should be encouraged to maintain and improve them. There is great scope in participative auditing and it has several positive features that can be summarized:

- It involves management in the auditing process as part of the team rather than using audit as a management spy. It is essential that the initial terms of reference and approach are discussed with management at the outset as this will set the tone for the resultant audit.

- It is not merely a question of being nice to the client as it has a more dynamic element that involves some flexibility on both sides. Artificial pleasantries are a far cry from working closely with a client in a problem-solving fashion.
- It can be more interesting in that it is not geared into error discovery and the audit findings are placed into perspective according to a clear prioritization process. The aim is not to report what was done wrong but more to report ways that management may better control their scarce resources.
- It can be more demanding where many complicated issues have to be built into the work and the auditor will have to decide how far to alter draft reports to reflect management's views. The great audit preserve, the audit report, is no longer sacred and bearing in mind that a report is simply a device for securing improvement, this should not pose a major problem.
- The results are discussed and agreed as the audit proceeds with regular interim reports and management may actually assist in developing proposed solutions. It is possible to present a record of control weakness to management at a wash-up meeting and work with them in completing the remainder, i.e. the necessary recommendations. This then becomes a true partnership with all sides having a major input.
- Managers are able to share their problems. It is also advisable to review the reports with lower levels of management. Working with the operational manager who is most in touch with the areas in question can be most rewarding. This is the person who will have to build on the recommendations that result from the audit. The participative style is designed to help develop the positive working relationships that would underpin such an approach.
- It can engender more commitment all round. Discussing the audit as it progresses brings all parties into the debate and, if carefully managed, can make everyone look forward to the resultant report.
- The auditor is able to address major issues. It is only by becoming involved in management's control problems that one is able to deal with high-level concerns. This process will bring a realism into the audit that allows the auditor access to the real problems, i.e. the important issues which in turn will raise the entire profile of the audit process.
- It promotes good co-operation between audit and management that can be used to build a client base across the organization. This in turn will engender a degree of support for the audit function that may be called on in times when central/support services are under financial constraints. The process of outsourcing (i.e. contracting out audit and other professional white-collar services) may also be confronted knowing that there is a committed level of support within the organization.

The Expectation Gap

External auditors are increasingly concerned about the expectation gap and this has received much press comment. For the external auditor there is little relief from the pressure to resolve this problem. This creates a perception that they should have a greater role in locating frauds and helping to sort out companies that are going wrong, despite the apparent healthy state of their financial statements. Internal auditors have a different problem in that we are able to adapt our role depending on what the organization requires. This could involve a flexible interpretation of professional standards but so long as we retain some audit work, many additional services may also be provided. It is the extent of these additional services and whether they interfere with an ability to provide an internal audit of the organization that is crucial. Neil Hodge has reported on

a recent survey. 'Understanding the Expectations of FDs Towards Internal Audit and Its Future', carried out by the consultancy, Business Risk Management:

> the perceptions on internal audit held by the FDs of the FTSE 200 companies is by no means universally positive. In fact, more than half the companies are either lukewarm or negative about the function and its contribution to the business. FD's comments about internal audit range from 'providing a value-added structure to the group' to 'useful low-key function' and having 'a rather slow and methodical image'. . . . The survey concluded with six main recommendations for internal audit:
>
> - enhance skills within the function and the quality of staff;
> - become more business/operationally oriented;
> - build a higher profile by linking in more directly to the organization's strategic objectives; be more proactive, responsive and innovative and measure the value added by the function much better.[22]

Client expectations of traditional internal audit services typically consist of:

- A check on remote establishments to ensure that they are complying with procedures.
- The investigation of frauds that they have been detected within the organization.
- Investigations into employees who cause concern to management in terms of breaching procedure.
- A continuous programme of checks over the output from various financial systems to assess whether these are correct.
- On-the-spot advice as to whether proposed management decisions are acceptable in terms of compliance with procedure and best practice.
- Ad hoc investigations requested by members of the corporate management team.
- Additional resources for computer system development projects.

The above creates a major problem for internal audit in that, on the one hand, we have to market audit services and as such define what the client wants. On the other hand, we have to retain the right to provide a professional audit service which means essentially advising on systems of risk management and internal control as a result of an agreed programme of audits. If we fail to respond to management expectations then this will put us at risk in the long term while if we carry out the above work, this turns us into management consultants. The rules to be applied to managing this situation may be set out as:

1. Isolate two ranges of clients. The audit committee who will be the client for audit work (risk-based systems auditing), and managers who can receive additional consultancy services.
2. Make sure the audit committee understands the concept of planned systems audits and that a basic block of resources must be reserved for this task.
3. Provide consultancy as additional services that are clearly distinguished from audit work. Ensure that management understands that they are responsible for compliance, information systems, fraud investigations and achieving VFM.
4. Publicize the audit role through suitable brochures, website presentations and correspondence.
5. Encourage managers to take a long-term view in promoting sound controls and so avoid the many problems that are derived from poor arrangements. This is a long process but is assisted by oral presentations in control that audit may provide to management.

If there is a situation where audit and consultancy services conflict in any respect, then ensure that the audit role reigns supreme. This is highly likely if the (broken) cycle is observed as in Figure 5.13.

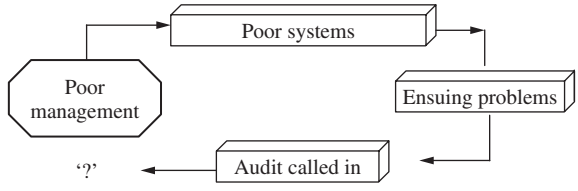


FIGURE 5.13 The control breakdown cycle.

The correct answer to the above scenario is that audit should seek to close the gap in controls that is caused by management's failure to establish sound controls. Chasing the results of control weaknesses (i.e. frauds, errors, poor performance, etc.) is in fact a poor use of audit resources. The worst scenario is where management purposely direct audit at fire chasing so that the auditor has no time to locate the source of the problems (i.e. management themselves). We may restate that reconciling these two issues is no easy task and involves:

- Keeping consultancy and audit services separate so that investigatory work done as a response to management's direct requests does not interfere with the ability to deliver planned systems assurance reviews.
- Making it clear at the outset that information from consultancy can and will be used in later systems work if there is a relationship.
- Making it clear at the outset that any breach of procedure identified during a consultancy project will be followed up and reported on separately.
- Where management has failed to install adequate controls and this is established via a consultancy project, this feature will also form part of the findings.

1. Time Busy managers find it difficult to assign time (and their staff's time) to deal with the auditor. Arrangements will have to be agreed to suit all sides and it is here that negotiation skills will come to the fore. The approach will have to be that audit will minimize interference with the work staff are performing and limit the time they spend away from their work. It is not good practice to abandon the audit since the current trend is for systems to be constantly under development and change. Audit must work within this environment and time and time again the auditor will start a meeting by being told that the manager only has a short time available, only to be discussing key issues several hours later. When a manager indicates that there are problems allocating time for the audit, what he/she really means is that there is little point spending resources in areas that have little or no return. Employing professional auditors who are asked to work to formal standards is one way of avoiding this. All managers encourage developments that help them achieve their goals and if audit have assumed this reputation then it will not be difficult to get cooperation from managers and their staff.

2. Terms of reference The opening terms of reference for the audit are always a difficult matter as each side feels the other out. There is always an element of suspicion from the client which itself is located in the whole issue of change management. The auditor must recognize the two main worries of the client:

- That the auditor may wish to recommend changes that will adversely affect the manager's position.
- That the auditor may in fact be investigating him, the operating manager.

3. Audit approach The audit approach and general attitude will have an impact on the resulting negotiations. It is generally accepted that negotiation is about compromise and securing benefits for all sides in contrast to a win/lose stance. There are auditors who feel that they work for a supreme force and must not back down to anyone. This is one reason why audit suffers a poor image as enforcers, although it is entirely the CAE's fault if audit staff are behaving in this fashion. Alicia J. Filak has discussed the issue of changing perceptions of the audit role:

> Auditors need to make every effort to promote mutual understanding between the audit department and the client. Although, many internal auditors may proclaim, 'We're here to assist you,' these words can be meaningless if the auditors do not truly value the client's input. We should always try to understand the client's point of view and approach each assignment as objectively as possible. Of course, mutual understanding can only be achieved if the other party grasps our point of view as well. By taking the time to explain the objectives of the audit and the benefits it may offer, auditors can help ensure that clients have a better appreciation of the purpose of our work and its value to the organization.[23]

4. Bottom line Sawyer's view of internal audit sees it as a function that seeks to leave the operation in a better position than it was before the audit. This does not mean that every detailed recommendation must be immediately implemented by management. It is based more on the view that management should be consulted and, where essential, they will take on board recommendations, although open to negotiation. It requires the auditor to negotiate recommendations and differentiate between those that are essential, important and merely useful. Using this approach, a little may be given up for the sake of progress in other areas.

The Link into Marketing

Marketing involves defining and then meeting client needs. Is this the case for audit services? To answer this question we need to consider the process in Figure 5.14.

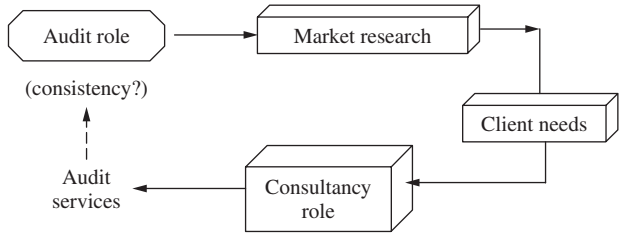


FIGURE 5.14 Marketing audit services.

This model would be perfect for most business units that exist primarily to meet a client's need. There is a nagging question mark near the top left-hand box that asks whether the type of services required by management is entirely consistent with the audit role. If not then we either:

1. fail to meet clients' needs, or
2. we must alter the audit role.

Each of these solutions goes on to provide further problems for the audit service that may eventually impair its efficiency and effectiveness.

One response to solving this problem is shown in Figure 5.15. The refinement to the original model means that we are now able to provide a consultancy-based service which can consist of any tasks/projects the client requires. This is in addition to our main-line audit role that necessarily requires us to:

1. define the audit field;
2. assess the relative risk of each 'audit unit';
3. draft a plan aimed at these high risk areas;
4. seek approval from the audit committee;
5. resource and implement this plan of audits that involves assessing the adequacy and effectiveness of systems of control in each material audit unit;
6. report the results to management and the audit committee.

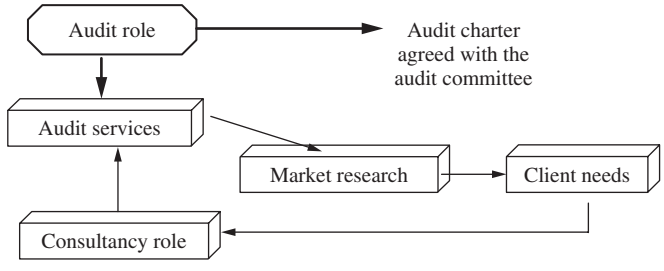


FIGURE 5.15 Marketing consultancy services.

Note that marketing is also discussed later in the Handbook.

Managing the Delinquent Manager

Much has been said about the need to feed the audit process into management needs and this is the only way for effective audit. This is because the business objectives are the paramount factors that drive the system and the subsequent systems' controls. Two other issues are: what to do about delinquent managers, and what to do in a corrupt organization. Delinquent managers may be defined as senior officers who are working to objectives that are inconsistent with organizational objectives. As they achieve their objectives, the welfare of the organization is impaired. There is little scope to discuss participative auditing and linking into managerial objectives. The difficulty comes in clearly identifying such people and either missing them or at the other extreme, assuming all managers fall into this category. If it is clear that a manager is acting in this way, the auditor must assume a reporting line with a more senior officer who is removed from this problem. The delinquent manager will seek to hinder the audit and get it aborted as a challenge to his/her position in the organization. The question of manager's needs does not arise as the auditor must rise above the operation and politics that will certainly confront him/her. The

auditor will be alerted and should carry out more detailed work into problem areas and report them to the most appropriate level of management. Where an entire organization is essentially corrupt, a whole new set of problems will arise. Returning to the lesser problem of the one-off delinquent manager, the following may be noted:

1. This problem must be discussed with the audit manager and an agreed departure from the participative approach will be required. The CAE should be kept informed.
2. The delinquent manager may operate a system of control that does not actually promote control so as to get around performance measures. This may typically include:
   - a lack of formal procedures;
   - an in-crowd of co-conspirators;
   - not being available to the auditor;
   - no clear accountability;
   - regular breaches of the corporate control systems such as the organization's revenue budgetary setting process or ordering procedures, etc;
   - a failure to respond to previous audit reports.

It may be possible to take disciplinary action against the officer in question particularly where breach of procedure has occurred. This factor should be discussed with senior management.

What About Independence?

We have highlighted the need to seek management support and apply high-level inter-personal skills. These skills do not come easily and there are still some auditors who stubbornly stick to the old-fashioned regime of viewing all employees as the enemy whose activities must be exposed (audited). This type of auditor will exhibit the following characteristics:

1. Almost non-existent communication with the auditee at operational level. The auditor appears almost as a spy, drifting into the relevant section, asking a series of blunt questions and then double-checking everything that he/she has been told. The auditor will restrict contact with operational staff unless absolutely necessary. It is almost as if the audit view will be tainted by anything that is disclosed by operational staff outside of formal interviews with the auditor.
2. Slightly more respect for senior management. This type of auditor quickly takes sides where senior management reflects the view that all their problems are caused by their staff. The audit becomes more of a check on the workers than anything else. There is no consideration of the principle that management is wholly responsible for the areas and staff under their control.
3. A view that all employees are guilty until proven innocent. Here one will look for noncompliance as the norm, based on the fact that most staff are not interested in their work at all. Taken to the extreme this results in a burning desire to identify wrongdoing whenever an audit is being conducted on the basis that this is the real audit role.
4. An intense resistance to discussing audit findings before they appear in a draft report for consultation. This auditor reports and runs. The report comes as a complete surprise to management as the findings have never been discussed or revealed. Communication is carried out through formal memoranda between auditor and client where points are raised and responded to.

This person achieved a basic distance from managers and operational staff that allowed him/her to act almost as an external review agency. The material on independence makes it clear that

performing low-level audits with no appreciation of business objectives militates against effective levels of independence in its wider sense. The question that arises relates to the difficult task of working among and with management, while still retaining some objectivity. There must be a limit on the extent to which we may cooperate with management since this impacts on the degree of objectivity. The more professional the manager, the less of a problem this poses as trained managers recognize the importance of sound systems of control and their responsibilities therein. Less able staff may not accept this principle, particularly where systems are weak and performance therefore suffers. The late Larry Sawyer has given some useful advice on managing relationships:

> The auditor must be prepared to manage the change resulting from recommendations or that are anticipated by the auditee. Following are several causes for auditee concern together with suggestions for palliative action by the audit staff:
>
> 1. Fear of the unknown can be neutralized by explaining the impact on current operations that the change will make and clearly describing the potential risks of the change.
> 2. Conflicts with present operations can be explained by describing the positive results that the change will make and the credits that will accrue to auditee management.
> 3. Ego problems can be resolved by bringing auditee management into the decision process so that the change actually becomes the product of present management.
> 4. Bureaucratic problems including the need for vertical and horizontal realignments can be reduced by working with all involved to outline the integrated changes that will be needed and by working with the horizontal and vertical units involved.
> 5. If the change is not cost beneficial or results in a less efficient operation, explain the positive results the benefits of which exceed the apparent losses.[24]

The behavioural aspects of internal auditing have been widely researched and it is clear that audit management needs to decide on which policies and procedures to promote based on the available options. Being nice is not enough and the audit department needs to identify management's risk management and control needs, explain how it can assist in solving control weaknesses and take management with it through the whole audit process. This must be done so that positive working relationships are established and maintained while at the same time preserving professional independence necessary to carry out good audit work. This is no easy task and requires commitment, training and practice. The auditor must recognize the importance and potential problems that one may encounter when dealing with people. The success of the individual audits and the whole audit role may depend on how this is managed. The organization and the auditor's own style will affect relationships and a team approach is helpful but can lead to becoming akin to a management consultancy service. The auditor must manage these relationships very carefully and apply professional skills and diplomacy in all circumstances. Auditors have great powers and may be misunderstood, although this will be partly the fault of the CAE if they operate under a cloud of mystery.

Giving Finance Dept. the Audit It Deserves

By Dan Swanson, *Compliance Week Columnist*

Usually I write about how to audit some aspect of a whole enterprise – say, how the company manages risk, or how executives invest their IT dollars. That's important. But we shouldn't lose sight of the nuts and bolts: Companies are run by specific departments doing specific jobs, and they need auditing too. So we're going to get back to our internal auditing roots this month, starting with the finance department. The finance function is critical because it helps drive most organizations to higher levels of

performance. A well-run finance department enables sound financial management, strategic planning, organizational performance reporting, treasury-related activities, and financial reporting (among many other things). It tells you how many dollars are coming and going and where they're coming from and going to. Without that information, people are driving blindfolded, and the organization will have a difficult time sustaining long-term value. The bottom line is that by focusing your audits only on financial reporting, significant activities within the finance function could be inappropriately or inadvertently ignored by executive management and the board. Key opportunities for growth and improvement could also be missed.

Characteristics of a World-Class Finance Organization

Where do you start? Obtain agreement on what the characteristics of a world-class finance function within your company should look like. Based on research published by the Government Accountability Office (GAO), ''the finance department'' can best be defined in terms of the business outcomes it produces – outcomes such as improved business analysis, innovative solutions to business problems, reduced operating costs, increase capability to perform ad-hoc analysis, and improved overall business performance. To build a world-class finance function and help achieve better business outcomes, organizations need to define the finance function's agenda – that is, get a consensus on finance's mission, vision, core values, and goals and strategies – and craft a plan to get there. The GAO has taken that high-level foundational effort even further, by outlining four broad goals and a total of 11 best practices that define a value-creating, customer-focused finance function that delivers real business results. They are:

(1) Make financial management an entity-wide priority.
    - Build a foundation of control and accountability;
    - Provide clear, strong executive leadership;
    - Use training to change the culture and engage line managers.
(2) Redefine the role of finance.
    - Assess the finance organization's current role in meeting enterprise objectives;
    - Maximize the efficiency of day-to-day accounting activities;
    - Organize finance to add value.
(3) Provide meaningful information to decision makers.
    - Develop systems that support the partnership between finance and operations;
    - Re-engineer processes in conjunction with new technology;
    - Translate financial data into meaningful performance information, (e.g. develop exhibits and dashboards that clearly communicate financial performance and its impacts on the organization).
(4) Build a team that delivers results.
    - Develop a finance team with the right mix of skills and competencies;
    - Build a finance organization that attracts and retains talent.

While many finance functions have been focused almost entirely on financial reporting – and make no mistake, that's a large and critical part of their job – a high-performance company needs to position the organization for the future, by building all the finance capabilities that are needed going forward.

Audit Finance to Improve Organizational Performance

Internal audit's evaluation of the finance function can provide valuable feedback to the board and executive management. An audit of the finance department should determine whether or not the function's current services are appropriate, whether performance is continuously being optimized, whether management and finance are working together, and whether finance is helping the company recognize and respond to new business opportunities as they arise. There are many issues worth exploring in an audit of finance; I present a few of the important ones below. The audit team will need to complete a comprehensive audit plan to determine the correct focus and priorities for an internal audit of the finance function. Remember, the goal of an internal audit should be meeting the assurance needs of the board and executive management.

Does the finance function help management define, and agree upon, strategy? Does it help with implementation of that strategy, including management's recognition of, and response to, new and emerging business opportunities? Auditors should investigate how accounting and operational performance data is being used to support budget formulation and strategic planning.

Do budgeting processes support the assignment of management accountability and monitoring of performance? The audit team should investigate whether the finance function helps top management with forward-looking analyses of the numbers and by forging strong ties between accounting information, budget formulation and capital investment, and strategic planning and implementation. A high-performance company needs to position the organization for the future, by building all the finance capabilities that are needed going forward.

Are there appropriate systems, policies, procedures, and guidelines relating to financial management? How successful is the finance department in meeting business needs? The audit could explore how much line managers value good financial management and information in the execution of their various duties. Managers must constantly leverage and make the ''best use'' of the monies, staff, and other resources they have under their responsibilities; deferring financial decisions to strictly the folks in finance is not a good practice.

Has the finance team done everything necessary to get a grip on the organization's financial needs? While everyone is trying to forecast the next disaster to ''handle,'' in my view, process improvement and constantly strengthening the company's key capabilities is a vital long-term approach to improving resiliency and overall performance.

Are all the finance functions performing well? The audit team should ensure the organization's functions have been defined: accounts payable, payroll, performance reporting, performance analysis, budgeting, and so forth. Confirm that assessment criteria are available to evaluate those groups' performance during the audit. A client satisfaction survey or formal external benchmarking could also be useful in completing an audit assessment of overall functional performance. Consider performing a strategic Strengths-Weaknesses-Opportunities-Threats (''SWOT'') analysis based on a portfolio of historical and plausible future events. The outcome of a SWOT analysis will identify specific and actionable key opportunities for improvements and growth.

Do the financial practices of the organization meet generally accepted and industry-accepted financial management standards? Compliance with accounting

and auditing standards is important, and an internal audit of finance should usually include a review of the organization's accounting policies and practices. Where departures in accounting policy or practice do arise – and sometimes an exception to common practice does make sense for a specific company – has that departure been explained and approved by the proper managers?

Organizations Must Proactively Improve Capabilities

An internal audit of finance should foremost identify key improvement opportunities. The audit should confirm long-term finance needs (financial management, treasury management, or anything else) are identified and being addressed. Equally important, the audit should make sure the finance department can track all the dollars floating around the company. Is cash management and bookkeeping strong? What can be improved?

Lastly, the audit should investigate who is driving organizational capability improvement efforts and assess whether those efforts are working well. Finance is not only about internal control over financial reporting, nor is it only about quarterly and annual reporting; while these activities are important, they do not significantly affect long-term value creation. A good finance function is about much more than that. A good audit of the finance function is about much more than that, too.

Reprinted from *Compliance Week*. This article was originally published in Compliance Week. Reproduced by permission of Compliance Week. All rights reserved.

5.8 Managing Expectations through Web Design

This section gives a brief review of some of the material that is being set up on internal audit websites. Most larger organizations have developed corporate websites that provide an open communications link between them and the outside world. Many of these websites drill down into separate areas for sections within the organization, including internal audit. The website material is also part of a more extended internal intranet. The CAE needs to consider carefully how to use this mechanism to communicate with stakeholders and internal customers, and help break down some of the mystique behind internal auditing. The internal audit website may be used to establish the role of the function and assist the task of managing expectations from people who may have a distorted perception of the audit role: as a basic checking function that examines the work of the finance staff and occasionally looks at operational records. A consideration of a sample of the websites of various internal audit shops makes for interesting reading. Some of the material that is being posted on these websites includes the following frequently asked questions (the reader may wish to choose some of these for their own website):

1. **Why this guide?** It is an idea to say why this information is being provided. Some audit shops suggest that the word 'audit' usually elicits some discomfort and we need to ensure there is no need for worry since audit aims to make a positive contribution. In years gone by internal audit used to look for mistakes and report these to senior management.
2. **What is internal audit?** Provide a formal definition of internal auditing that makes sense and fits the organization. Perhaps the IIA definition, then a short, user-friendly explanation of some of the components.

3. **What is the overall mission statement?** This may be a short statement that has been agreed as the overall mission – perhaps linked to promoting good corporate governance and risk management in all levels across the organization and providing independent assurances.
4. **What is the internal audit's vision?** Some audit shops develop a vision of what they would like to be in the future as, say, having helped develop a committed workforce who have got to grips with the demands of good corporate governance.
5. **What is the audit objective?** This part will say what internal audit is trying to achieve and may be a mix of consulting roles in helping management understand and manage their risks, along with an assurance role of providing impartial assurances to the board and audit committee that controls are in place and working.
6. **Why do we have internal audit?** This provides an opportunity to note the benefits from internal auditing without going over the top. Some measure the success of internal audit in terms of the development of a sound control environment within the organization.
7. **Who are the internal auditors?** It may be possible to say who exactly works in internal audit along with thumbnail photographs.
8. **How are we organized?** Provide the authority mandate (laws, regulations, listing rules and so on) and then the organization chart with the CAE, reporting lines and then make reference to the audit charter. Specialist areas such as financial, information system audits, fraud, CSA, other consultancy services and so on may be listed.
9. **what is the difference between the audit and management role?** It may be possible to describe managements' responsibility for ensuring sound systems of internal control that mitigate unacceptable risks and then the internal audit role in adding value to this task and providing independent assurances. Mention management's responsibilities to cooperate with the internal audit process.
10. **What is the difference between external and internal audit?** Make clear these differences and explain that we try to coordinate efforts wherever possible. It may also be an idea to mention other review and inspection teams that may visit parts of the organization. Advise a protocol for clarifying which team the visitor comes from by suggesting that the manager ask questions to determine which team is carrying out the review. Suggest a reporting procedure where the manager feels there are too many different review teams visiting and therefore excessive duplication and interruption. Make clear that internal audit is a high-level function that also audits other review and compliance teams.
11. **Why do we need internal audit?** Describe some of the advantages in having good risk and compliance systems and an overall sound system of internal control, the internal auditors are a source of expertise in these somewhat complicated areas. We are all on the same side in seeking to ensure there are no material weaknesses in systems of internal control.
12. **How is internal audit independent?** Outline the concept of independence (status and objectivity) and that internal audit work can be relied on as professional, impartial and reliable.
13. **How does the audit committee come in?** Outline the role of the audit committee and the types of support, plans and reports that are provided by internal audit to help them discharge this role.
14. **Where does internal audit authority come from?** State the source and explain where the audit charter can be viewed. Make it clear that internal audit operate to professional standards. Say that internal audit have access to all information, explanation, records, files and buildings to perform audit work.
15. **What is the scope of audit work?** Describe the components of VFM, information, safeguarding assets and ensuring compliance. Mention corporate governance, risk management

and internal control, along with other aspects such as fraud, IT audits, CRSA and staff awareness seminars and guides.

16. **What does internal audit do?** List in more detail the services that are provided by internal audit, including ongoing advice and assistance. Make it clear that auditors spend a lot of time interviewing staff and analysing records and information. They are not checking on what staff do, they are checking on the system for managing risks to the operation. Although audit standards tend to mean anything that is presented to the auditor may need to be confirmed before it is accepted as evidence.
17. **How are areas selected for audit?** Set out the risk-based planning process and the way audit plans are aligned to the risk exposures in all parts of the organization. Define the role of the board and audit committee in agreeing these plans, and the consultation process involved before the annual audit plan is adopted. Essentially we focus on high risk areas. If cyclical audits are still undertaken then describe the areas covered, such as cash, payroll. It may be possible to mention the key audit priorities for the current year.
18. **How does internal audit fit in with risk management?** Make it clear how internal audit fits in with overall risk management. Audits are not responsible for managing business risk but will have various degrees of involvement from setting up the systems to facilitating risk workshops to review the process in hand – whatever the format, internal audit will still give formal assurances on the system and reports any gaps and weaknesses.
19. **What is CRSA and do we not do our own audit using this tool?** Tell the reader about CSA (or CRSA – or whatever it is called in the organization). It is a good idea to have a guide (two to three pages) on the intranet, or available in hardcopy form. Some internal audit shops will present the guide to group meetings of staff annual conferences on request. CRSA does not replace an audit but it is an attempt to get business risks understood, assessed and then managed by those responsible for the process in question. Internal audit may help with this process or may use the results as a head start into their independent review based on sound evidence.
20. **Does management have any involvement in setting audit terms of reference?** Make it clear that the audits are taken from the audit plans and advance notice is provided (say 1–4 weeks in advance) and that the auditor will do some preliminary work before the initial meeting. The manager's views will be taken into consideration before finalizing the audit terms of reference and this will happen after the opening meeting (which may also involve touring the facilities and considering the manager's risk register).
21. **What if you feel you do not need to be audited?** The preliminary survey will help determine the terms of reference and in rare cases it may not be necessary to go ahead with the audit. Where the client feels that there is no need, it is unlikely that the audit will be cancelled, but the audit work may be reduced where there is sufficient reason.
22. **How can you facilitate the progress of the audit?** Internal audit work in partnership with management and their staff and the audit will go smoothly if there is good cooperation. Making time, space and information available to the auditor beforehand will help progress the work. Assigning a staff member to deal with requests from the auditor is another good idea. The auditor is used to working with busy people and will try to minimize disruption. The audit policy suggests that the real benefits from the audit will mean it is seen as worth spending time on.
23. **Do we have any set values?** Mention any agreed values such as integrity, honesty, excellent service, respecting clients and others. Also that audit will be conducted with due regard to set protocols (refer the reader to a separate paper on the audit process).

24. **What are the professional standards?** Mention the fact that internal audit subscribe to professional standards (e.g. IIA) and that the audit manual reflects the way the requirements of these standards will be discharged.
25. **What takes place during an audit?** Define the audit process, e.g.:
    1. notification
    2. entrance conference
    3. terms of reference confirmed via risks that have been identified
    4. fieldwork and data gathering and testing
    5. discussion of findings as they arise
    6. quality review of audit work
    7. closing conference – all findings discussed in outline
    8. draft report
    9. may make formal presentation to your management team
    10. response to report within 15 days – we will take on board points raised
    11. action plan
    12. final report
    13. customer survey – feedback on how you found the audit in terms of performance and end result
    14. follow-up within 12 months of the audit
    15. quarterly summary report to audit committee.

    An alternative approach will be to carry out a CSA workshop at stage 3 to determine operational objectives and assess the risks that need to be addressed. These risks are considered during fieldwork through a clear testing strategy. Then discuss audit findings at stage 7 and work with the management team on a sensible outline action plan.
26. **How long do audits last?** Depends on the type of audit, significance of risks and what is found. Can last between (put in a figure) e.g. one and two weeks, two and four weeks, etc.
27. **What is audit testing?** Describe the testing approach and that audit have moved away from blanket testing to risk-based audits and very selective testing. Explain that audit findings should be based on sound evidence.
28. **What occurs after the audit?** Describe the report clearance process from draft to final and that comments will be incorporated into the report or added as an annex. Discuss the follow-up audit and what happens to the audit report. The main thing that happens after an audit is action to put right any weaknesses, and the receipt of formal assurances from the internal audit where controls are sound. All agreed audit recommendations need to be implemented unless there is good reason not to.
29. **Where do the reports go?** Explain the protocols and who receives copies of the report, such as directors, board members, audit committee on request, external audit, management team, etc. Less material matters may go into a memo to the line manager. Public bodies may post the audit report on the organization's website. External parties such as regulators may have access to the reports if required.
30. **What are the follow-up procedures?** Describe the follow-up procedures and that more work will be carried out on more significant findings to address outstanding risk. Crucial recommendations may have to be acted on urgently.
31. **Do we accept requests from management?** Describe the criteria for deciding whether or not to perform any formal consulting projects that are requested by management. This may include assessment of the following:
    - material risks involved

- previous efforts to address concerns
- related to risk, control and governance issues
- no audits scheduled in the areas for a while
- audit has expertise and time available
- board (or senior management) endorse the request
- major impact on achievement of corporate (or department) objectives
- problem impacts on reputation of organization
- previous audit work on similar problems has proved successful
- audits have access needed for this type of work
- high level of sensitivity required
- importance of impartiality of reviewer
- other special factors.

32. **What do managers need to know about risk and controls?** Some audit shops prepare a guide to internal control that can be downloaded for use by managers and work teams. Other audit shops offer staff awareness seminars on risk management and internal control.
33. **Do we conduct surprise audits?** If this rather old-fashioned technique is still used, explain why and how it is conducted for, say, cash funds, accounting records, employee records, observation of operations, inventory records and so on. If surprise audits are no longer used, make this clear because many people do not realize that internal audit have generally moved on from being a hit squad.
34. **What do we do about fraud?** Describe the fraud policy, audit's role in respect of fraud and the reporting system for suspicions. This should all be in the separate fraud policy, available to staff. Make it clear that management is responsible for dealing with fraud but may seek help from specialist staff.
35. **What does internal audit not do?** List some of the line roles that audit used to do but have since dropped. Some say that audit will not tell management how to do its job, but simply use audit expertise to help management discharge its obligations in respect of risk management, control and governance processes.
36. **Who audits the auditors?** Outline the quality assurance regimes of internal and external review, supervision of audits and setting and reporting on performance measures. Mention that the audit committee monitors the work of internal audit and each auditor accounts for their time and performance through a highly developed MIS (time recording and accounting).
37. **What are the Complaints procedure?** Describe the complaints procedure and say that internal audits work to the highest professional standards in adding value to the organization and that we welcome comments and suggestions. Give the reader a contact point.

5.9 Audit Competencies

We have covered the role and responsibilities of the internal auditor and the tremendous challenges facing the new-look auditor in the continual search for better and more effective corporate governance arrangements. One aspect of these challenges that is often overlooked is the need to ensure the audit staff are equipped to work at sub-board level, that is, right near the top of huge international organizations. The new-look internal auditor has to be totally competent or they will fail miserably. IIA standard 1200 deals with proficiency and due professional care by stating that:

> Engagements must be performed with proficiency and due professional care.

While standard 1210 covers proficiency in more detail:

Internal auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively must possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities.

Interpretation:

Knowledge, skills, and other competencies is a collective term that refers to the professional proficiency required of internal auditors to effectively carry out their professional responsibilities. Internal auditors are encouraged to demonstrate their proficiency by obtaining appropriate professional certifications and qualifications, such as the Certified Internal Auditor designation and other designations offered by The Institute of Internal Auditors and other appropriate professional organizations.

What makes for Good Internal Auditors

The first thing that needs to be in place to ensure good internal auditors is effective human resource policies and practices. Here we are concerned with the attributes of successful internal auditors. The IIA Practice Advisory 1210-1: deals with proficiency and requires that each internal auditor should possess certain knowledge, skills and other competencies:

- Proficiency in applying internal audit standards, procedures, and techniques in performing engagements. Proficiency means the ability to apply knowledge to situations likely to be encountered and to deal with them appropriately without extensive recourse to technical research and assistance.
- Proficiency in accounting principles and techniques if internal auditors work extensively with financial records and reports.
- Knowledge to identify the indicators of fraud.
- Knowledge of key information technology risks and controls and available technology-based audit techniques.
- An understanding of management principles to recognize and evaluate the materiality and significance of deviations from good business practices. An understanding means the ability to apply broad knowledge to situations likely to be encountered, to recognize significant deviations, and to be able to carry out the research necessary to arrive at reasonable solutions.
- An appreciation of the fundamentals of business subjects such as accounting, economics, commercial law, taxation, finance, quantitative methods, information technology, risk management, and fraud. An appreciation means the ability to recognize the existence of problems or potential problems and to identify the additional research to be undertaken or the assistance to be obtained.
- Skills in dealing with people, understanding human relations, and maintaining satisfactory relationships with engagement clients.

Skills in oral and written communications to clearly and effectively convey such matters as engagement objectives, evaluations, conclusions, and recommendations.

The organization of the future will be a conveyor of ideas, with the sourcing of products and services a secondary issue. The customers says what they want, and the organization delivers.

Meanwhile, the organization also helps the customer raise their sights in envisioning what is available. In this way, the organization of the future is a collection of visions and intellects brought together by a dynamic information and communications network. The importance of getting the right competencies in staff has never been more crucial to business success, and internal auditing is no exception. Some of the attributes that the competent internal auditor needs to demonstrate include the following (in no particular order):

- able to apply innovative and creative thinking;
- able to work to agreed timescales and account for time;
- able to add value to the organization;
- able to appreciate concerns of stakeholders and focus on needs of the customer;
- able to appreciate new ideas and embrace and encourage change;
- able to establish credibility with senior management and at grassroots;
- able to function within flexible working arrangements;
- able to plan work and have a sense of urgency in performing the audits;
- able to quickly build relationships but retain professional stance;
- able to work under pressure and set priorities;
- ambitious and confident without being overbearing;
- appreciation of business environment and new ventures;
- balance and common sense with an overall sense of fairness and diplomacy;
- can cope with travel requirements and overnight stays;
- commercial awareness;
- committed to continuous learning and open to training and development;
- committed to working within set corporate policies and section procedures;
- communications skills, oral, public speaking, writing, report writing, effective listening, written and inter-personal skills at all levels;
- diplomatic but persistent where required;
- emotional intelligence and good balance of emotions such as anger, sadness, fear, enjoyment, love, surprise, disgust, shame – and humility. The ability to apply social skills such as trustworthiness, empathy, adaptability;
- enthusiastic, task-oriented person, able to focus on the job in hand;
- facilitation skills with an emphasis on challenge and co-ordination;
- formal report writing;
- general management skills and able to provide direction, delegate and monitor results through performance review;
- global perspective and interest in international developments;
- good balance of consulting and assurance approaches and able to reconcile possible conflicts between helping people and reviewing systems;
- good decision making and judgement with no special bias to self-interests;
- good interviewing technique and able to empathize with the client;
- good problem solver and able to weigh up pros and cons of different options and to see around the problem through to solutions;
- intellectual capacity and able to see things for what they are and ascertain causal relationships between problem, cause and effect;
- appreciative enquiry – looking for the positive in human undertakings based on the great energies that come from success and accomplishments;
- inter-personal skills recognizing group dynamics and people behaviour;
- leadership and drive with a clear sense of direction;

- mature and professional enough to deal with different types of people and operate across different cultures;
- negotiation skills and some tenacity in sticking to crucial points;
- objectivity and independence with an ability to remain impartial;
- practical edge in applying policy and an understanding of any limitations;
- presentation skills;
- project management skills;
- self-motivated with good initiative, and enthusiastic even when performing mundane tasks;
- some commitment to developing a career in internal audit;
- task-focused and good at applying energies to delivering results;
- team player – able to buy into team working and team tasks with an understanding of the importance of being friendly, participative and helpful, and having fun where possible;
- basic technical skill – financial, legal, economics, accounting, auditing, computing, statistics, other analytical techniques, database and spreadsheet use, data interrogations and so on;
- track record of achievement and completion of tasks;
- understanding of modern audit techniques including corporate governance, risk management and control;
- understanding of internal audit procedures and quality requirements;
- understands big picture but can respond to detail when required, notwithstanding apparent ambiguity.

The new look creates a very demanding role. It includes all those aspects that make a good traditional auditor with a hard nose and deep concern with getting to the truth, and the new approach of being a top flight consultant on risk and control issues. A job advertisement for European Commission – Deputy Director for Audit includes the following extracts:

> Have the necessary professional competencies and in particular have a social auditing background as well as a sound knowledge of internal control frameworks, and management techniques. Be able to demonstrate:
>
> - the necessary personal qualities and excellent management skills for a complex multicultural environment.
> - excellent intellectual, communication and interpersonal skills.
> - proven ability to take a leading role in developing and supporting an active, strategic and modern Internal Audit Service.

Continuous Professional Development

Having got the right audit staff in post, it is then a question of getting them to perform and ensuring that they continue to develop. The IIA Attribute Standard 1230 on continuing professional development (CPD) requires that:

> Internal auditors must enhance their knowledge, skills, and other competencies through continuing professional development.

The IIA Practice Advisory 1230-1 continues this theme and suggests that:

> Internal auditors are responsible for continuing their education to enhance and maintain their proficiency. Internal auditors need to stay informed about improvements and current

developments in internal audit standards, procedures, and techniques, including The IIA's International Professional Practices Framework guidance. Continuing professional education (CPE) may be obtained through membership, participation, and volunteering in professional organizations such as The IIA; attendance at conferences, seminars, and in-house training programs; completion of college and self-study courses; and involvement in research projects.

Internal auditors are encouraged to demonstrate their proficiency by obtaining appropriate professional certification, such as the Certified Internal Auditor designation, other designations offered by The IIA, and additional designations related to internal auditing.

Internal auditors are encouraged to pursue CPE (related to their organization's activities and industry) to maintain their proficiency with regard to the governance, risk, and control processes of their unique organization.

Internal auditors who perform specialized audit and consulting work – such as information technology, tax, actuarial, or systems design – may undertake specialized CPE to allow them to perform their internal audit work with proficiency.

Internal auditors with professional certifications are responsible for obtaining sufficient CPE to satisfy requirements related to the professional certification held.

Internal auditors not presently holding appropriate certifications are encouraged to pursue an educational program and/or individual study to obtain professional certification.

Marion Lower has prepared guidance on CPD (CPD – Learning for the Longer Term 2002) for the IIA.UK&Ireland. The guide promotes CPD as a way of optimizing career opportunities by demonstrating and maintaining high levels of professional competence through continuous upgrading of skills and knowledge. The audit process is seen as consisting of:

- understanding the organization's exposure to risk;
- understanding how those risks are managed by controls
- improving risk and control systems;
- providing assurance on risk and control systems;
- managing the internal audit process and function.

Three levels of internal auditing skills are detailed, consisting of entering, competent and audit manager levels. For these three levels, standards are set for cognitive skills (technical skills, analytical/constructive skills and appreciative skills) and behavioural skills (personal skills, inter-personal skills and organizational skills). The CPD process consists of three main stages:

stage 1 – analysis of personal skills and work experience, identification of career opportunities, threats which might prevent these being secured. Then review with line manager or mentor.

stage 2 – building a professional development plan.

stage 3 – maintaining a professional development diary.

Some of the aspects of development would include the following:

- Professional – IIA committee work, lecturing, examining, authoring articles, attending District meetings.
- Educational – masters degree in internal auditing, MBA, other certificates/diplomas.
- Training – attendance at short courses, seminars and conferences.
- Work-based development – projects, secondments.
- Self-directed learning – reading books, journals, etc., audit related audio/video tape, technology-based training packages.
- Other activities – voluntary work.

Competency Framework for Internal Auditors (CFIA)

There really is a call for a 'new look' internal auditor. The best way to convey this viewpoint is to refer to the words of Bruce Adamec, as recounted by Michale Barrier:

> Internal auditing became a dumping ground, Adamec (Bruce Adamec, General Auditor of Ameritech) says because, ironically, it was regarded as so demanding. 'For the first two years you worked in the department, you were not allowed to do productive work because you were told you were not qualified,' he explains. 'You set expectations like that, and basically, people work to those expectations.' Such a conception of internal auditing made no sense to Adamec. By 1990, drastic changes in technology had paved the way for even inexperienced internal auditors to play a significant role almost immediately. So Adamec began shaking up the department, cutting the total staff in half, to about 75 people. He cut managers, supervisors, and team leaders getting rid of 'a lot of people who specialized in finding mistakes, or "gotcha" auditing'.[25]

The IIA undertook landmark research into audit competencies via a research team that included William P. Birkett, Maria R. Barbera, Barry S. Leithhead, Marian Lower and Peter J. Roebuck who sought to address four main questions:

1. What is understood by internal auditing in the future, from a global perspective (what is internal auditing becoming and what is it to be)?
2. What are the attributes of a competent (quality) internal auditing function within organizations from the perspective of best practice globally?
3. What capabilities are to be required by those taking key roles in a competent internal audit function?
4. How is the competency of an internal auditing function and the capabilities of those taking key roles best assessed?

Competency Framework for Internal Auditor (CFIA) (*Structures and Methodologies* booklet, page 60) has developed a skills taxonomy covering:

1. **Cognitive skills:**
   - Technical – communication (ideas, reports, presentations), numeracy, computer literacy, internal auditing technologies.
   - Analytical – research/reasoning, organizational analysis, systems design.
   - Appreciative – discrimination (e.g. knows when to ask questions), value orientation (appreciates training, quality, challenge, etc.), judgement.
2. **Behavioural skills**
   - Personal – morality, directed, inquisitive, flexibility, coping, intelligence.
   - Inter-personal – communication, people skills, team management.
   - Organizational – organizational awareness, functional management (for internal audit), organizational management.

These are applied to three categories of internal auditors:

1. entering internal auditor
2. competent internal auditor
3. internal audit manager.

One of the authors of CFIA, Barry S. Leithhead, has put the new competencies into perspective by relating them to the paradigm shift from old- to new-look internal auditing:

Major paradigm shift:

from	to
control	risk
risk	contexts
past	future
review	preview
current	concurrent
independent	value
audit knowledge	business knowledge
audit operations	audit strategy
imposition	invitation
persuasion	negotiation[26]

The CFIA study focuses on 6 *Units of Competency* and 27 *Elements of Competency*. A *unit of competency* is the set of tasks needed to meet the functional requirements of a type of work. The six *units of competency* are

Unit 1 – Develop *understanding* within an organization about the risks associated with its functioning and contexts.

Unit 2 – Develop *understanding* within the organization about the *adequacy and effectiveness of its control strategie*s, structures and systems.

Unit 3 – Contribute to *improvements* in the functioning of the organization's risk management and control systems.

Unit 4 – Provide *ongoing assurance* to the organization that it is in control relative to its risks.

Unit 5 – Manage the internal auditing function.

Unit 6 – Manage within the dynamic contexts that affect the work of the function.

One key point made by CFIA is that: 'the notion of internal auditing as a constant, independent appraisal function may become passé. Rather, it will be seen as a mechanism for providing assurance that risks are correctly understood and managed in the midst of dynamic organizational change.' This has been a main driver in the growth and importance of the internal auditing role and the fact that it is now recognized as one of the cornerstones of corporate governance. More and more regulatory codes are making it clear that large companies and bodies should really have a fully equipped internal audit function. CFIA moves this proposition forward by arguing that 'Internal auditing is a process by which an organization gains assurance that the risk exposures it faces are understood and managed appropriately in dynamically changing contexts.' And that the value proposition for internal auditing is contained in the outcomes of its work and the quality of the processes by which the work is performed. Outcomes can be described in terms of the services provided, such as assisting in managing risk, promoting effective control, and providing quality assurance. The IIA has developed competency frameworks that encompass inter-personal skills and knowledge areas required to varying degree from auditors depending on their grades which range from CAE, audit managers, seniors and juniors through to new audit staff. The inter-personal skills cover areas such as:

INFLUENCE: Wielding effective tactics for persuasion

COMMUNICATION: Sending clear and convincing messages, listening

MANAGEMENT
- policies and procedures
- staffing
- priority setting, planning, performance management and customer focus
- time management, achieving goals and tasks and organizational skills.

LEADERSHIP: Inspiring and guiding groups and people, building organizational commitment, and entrepreneurial

CHANGE CATALYST: Initiating, managing and coping with change.

CONFLICT MANAGEMENT: Negotiating and resolving disagreements.

BUILDING BONDS: Nurturing instrumental relationships, working with others toward shared goals.

COLLABORATION AND COOPERATION: Working with others toward shared goals.

TEAM CAPABILITIES: Creating group synergy in pursuing collective goals.

5.10 Training and Development

Training is an important aspect of developing internal auditors, and has to be carefully planned in line with a career developmental programme. Several issues should be noted.

Common Body of Knowledge

The IIA has developed 20 disciplines in order of overall perceived importance:

1. Reasoning
2. Communications
3. Auditing
4. Ethics
5. Organizations
6. Sociology
7. Fraud
8. Computers
9. Financial accounting
10. Data gathering
11. Managerial accounting
12. Government
13. Legal
14. Finance
15. Taxes
16. Quantitative methods
17. Marketing
18. Statistics
19. Economics
20. International

IIA.UK&Ireland Syllabus

The year 2002 saw the introduction of a new syllabus for the IIA.UK&Ireland that sought a wider coverage of the audit world and related areas. This now provides two levels of qualification, the practitioner level (Diploma in Internal Audit Practice – PIIA) and the more advanced professional level (Advanced Diploma in Internal Audit Management – MIIA). The professional level builds on and extends the subjects that are covered at practitioner stage. Besides internal auditing topics, there is coverage of financial and general management, information systems and a new module dedicated to the topic of corporate governance and risk management. The advanced internal auditing paper is based around a case study that is available before the

examination date, so reflecting the growing trend towards more practical work. The PIIA topics are: organization and management, accounting and financial systems, internal auditing, business information systems auditing, and corporate governance and risk management. The MIIA topics are: advanced management, financial management, advanced information systems auditing, and advanced internal auditing. There are also two skills modules that the students are required to complete on communication and client/auditor relations and effective delivery of an audit. More recently, the IIA.UK&Ireland have developed a certificate in Corporate Governance and Risk Management.

As well as formal qualifications, there is an entire spectrum of developing people at work that includes:

- Training – programmes for getting people learn to do things differently.
- Development – untaught activity to increase/improve performance.
- Education – formal courses to develop knowledge and qualifications.
- Learning – acquiring better skills, knowledge and attitudes.

Benefits of Training

Increase in the quantity of work done by auditors Audit training is not carried out for its own sake but should be designed to secure defined benefits. There should be an increased efficiency in the way audit work is carried out which is then translated into increased output. A suitable training programme may have as an objective the reduction of audit hours charged to planned audits so that in any one year, more audits may be completed. Better techniques and more efficient procedures should lead to higher turnover.

Better quality of work It is one thing to churn out audits, and performance indicators based on this sole factor will be misleading. Audit training should achieve a higher standard of quality from auditors. Training may have a firm objective to produce excellence. There should be a direct link between the level of training and the increasing ability to audit at higher managerial levels.

Cost savings in terms of better overall performance Becoming more efficient can be translated into the number of audits performed in any one period. On the other hand, it may also be seen in terms of the potential to effect cost savings. It is possible to get more junior staff to operate unsupervised through effective training so that the overall charge to an audit will include less time from the audit managers. One useful technique is to move away from audit teams and get each individual auditor to perform his/her own audit project.

Better standard of report writing This is more a process for change than a mere document. Some argue that the report is the 'window' to the audit department as a formally published item widely read. There is no short-cut to performing good audit work and this should be the main concern of audit management. Much will be lost if this professionalism is not wholly reflected in the final product, i.e. the audit report. It is here that additional effort must be expended to complete the circle of performing good work and then reporting it. Audit training will certainly include report writing, and inconsistencies between individual auditors will arise. Some of these are not only attributable to junior staff but will also cover different reporting styles acquired over time that need to be harmonized. Reference to the audit manual will help define the reporting standards that have been adopted, bearing in mind the fact that there are many different models that may be applied.

Better quality of working papers We are moving to a position where the working papers that are prepared by auditors are acquiring a clear status. The rules on advance disclosure of evidence, and public enquiries that may be commissioned in the public sector as well as by the regulatory agencies in the financial services arena, mean that audit findings may be subject to an independent third-party review. Audit's quality assurance provisions will also require formal standards that cover audit working papers and these should be properly implemented. Whatever the scenario, there is a need to ensure that auditors are preparing suitable working papers. It is frustrating to review a report that is well presented and based on sound evidence but the underlying evidence cannot be readily gleaned from the working paper file. It is here that many auditors let themselves down. A formal standard on audit documentation must form part of the audit procedures and its implementation will necessarily include training sessions on this topic, again based around the audit manual.

Less audit staff required in the long term This is a sensitive topic but one may assume the stance that training will help produce a higher standard of auditor which in turn should generate better work. One useful model is to employ a smaller number of auditors, working to higher standards. This does depend on the type of work being carried out, although if facing competition, as is the case in the public sector, then this 'downsizing' is a fact of life. Training facilitates this process as skills are spread, greater efficiency is encouraged and the training process itself may be used to filter out those staff who are not able to readily transfer to these higher standards. If one has to be cynical, it should be noted that it is not best practice to take action against staff who are not performing unless relevant training programmes have already been directed at these staff. The process of defining a training programme necessarily involves setting performance standards and if an auditor is not able to meet these after all available assistance, management must then review this individual's position.

Smaller training gap in terms of skills shortages The audit manual will set standards covering the way that the audit role is discharged in a particular organization. This will be designed to promote efficiency and effectiveness and so help guarantee the future of internal audit. Within this thinking is the presumption that all audit staff are able to function to the various standards that have been adopted and there will be obvious problems where this is not the case. A skills gap exists when auditors are not able to meet management's expectations and again if this is the case, the audit manual may fail. It is essential that all skills gaps are systematically identified and closed through a suitable training programme. All training should have this clear objective and so runs the argument that as these gaps are closed, audit will be better able to succeed.

Greater degree of professionalism Throughout the handbook we have developed a model that views audit as assuming a greater degree of professionalism with the passing of time. This is a conceptual matter that runs across the whole discipline of internal auditing. In practice, however, it has to be translated into the work being carried out in each individual audit department and it is here that training comes into the frame. Training will play a major role in making progress towards this model of smaller numbers of more professional auditors. This is in contrast to vast armies of junior checkers that was a feature of the old days of internal auditing. Training is not only seen as a way of effecting development but can also comprise a set of basic targets that must be achieved before we can start to talk of this development. Herein lies the argument for using qualified staff.

Better motivated workforce with career development programmes Training means more than mere courses, seminars and days out. It indicates commitment from audit management

to staff and injection of resources for each employee. Where training is linked into individual career development programmes, which is really a necessity, then it will have a motivating effect all round. It is possible to build team association into training by working on case studies in small groups and so enhancing the ability of staff to work together on real-life audits. Whenever a course is organized, the impact on motivation should be considered and catered for in the course wherever possible. For external courses, an example would be to arrange them at a scenic location and have staff travel there together (say in one car). In this way, it acts as a team-building day out in addition to the dissemination of information. Without a suitable training programme, performance appraisal has little use as there is no point identifying a skills gap and then not seeking to close it. In this instance, an appraisal scheme would probably act to demotivate participants and lower performance. Motivated staff are more likely to stay with the audit team for longer and this factor should be considered as part of an overall staff retention strategy. The World Bank's approach to staff retention includes:

- treating auditors as independent consultants
- giving them responsibility for their careers
- training and development
- challenging assignments
- client liaison responsibility[27].

Training Auditors

1. Specialist skills training via internal or external skills workshops These can be extremely efficient in terms of auditor development as long as the following rules are adhered to:

- They are tailored to the exact requirements of the internal audit department in question and not framed as general developmental courses. There is little point having a trainer stand in front of an audit team who has no idea what specialist work this team is involved in.
- They form part of an individual auditor's career development programme and can be geared towards tackling known weaknesses, identified from the performance appraisal scheme.
- They are based around a needs analysis that has formally identified the training needs of the department.
- The matters set out in the course are immediately put to use in a practical way in current audit work. This is a major benefit in that the real training goal is achieved not when participants listen to a trainer, but when they actually perform the new techniques learnt.
- There is a clear link into the performance standards as set out in the audit manual. Skills workshops may be used to reinforce the standards required by the audit manual, which will encompass the defined working methodologies that have been adopted by the audit unit in question.
- They form part of a formal ongoing programme that falls within the strategic goals of the audit department, as a way of ensuring that staff understand and work within the frame established by the strategy.
- The workshops may be supported by audit management who may assume a key role in delivering the training modules.
- The policy may be to utilize all available in-house skills before external sources are applied to this programme. This is why the skills database that was discussed earlier is useful in isolating in-house skills and ensuring that they are shared.

- If the skills workshops are performed by external resources, they should be based on a tailored programme specifically designed by audit management.
- The CAE takes a personal interest in these programmes and ensures that they are given a high profile in the audit strategy. One major benefit of the skills workshop approach is that they may be contained within the working day. So, for example, we would expect audit management to introduce a 2-hour session to cover a new development that will consume very little audit hours, or interfere with ongoing audit work. This means there is no reason why this type of training should not be undertaken frequently, whenever there is a need.
- VFM is achieved from them in terms of their transition from classroom to their successful application to audit work.

2. Professional training This may be based on passing examinations of a defined professional body such as the IIA, which is a completely different form of training from skills-based courses. As such, the rules here are different:

- This must form part of a long-term strategy underpinning the entire staffing policy of the audit department. It takes years to put staff through professional courses and a long-term approach is essential for this policy to become successful.
- A formal budget must attach to this programme that caters for subscription fees, books, travelling, college fees, time off, exam fees and so on. The CAE must be wary about depending on corporate training budgets as these tend to suffer in times of budget reduction exercises. As such, the CAE may wish to set aside a separate fund for this activity financed by fees from additional areas such as consultancy services.
- The requirement to secure a professional qualification should form part of the staffing policy. Real success is achieved when auditors are required to pass the internal audit qualification, to remain with the organization or at least obtain internal promotion. Unfortunately, it is only by placing this severe pressure over the career auditor, that one can guarantee that studies will be prioritized, so making success in the ensuing exams more probable. Without this pressure, much is left to chance and many auditors will not study sufficiently hard to pass the exams.
- Professional exams cannot replace skills workshops for a number of reasons. First, they are based on general concepts and not geared towards any particular audit methodology. Second, it does not train individual auditors based on their special training needs but simply conveys the basic principles of best audit practice. Lastly, an auditor who is well versed in 'question spotting' can pass a variety of exams without really understanding much about the topic in question.
- Audit management must have a mechanism to enable any elements of best professional practice, which is learnt in a classroom and brought back to work, to be considered and catered for within the audit department. An example may be statistical sampling which may or may not be applied by the CAE, but cannot simply be ignored.
- The policy on audit textbooks should ensure that they are acquired for the department and not the individual, and sufficient copies are made available to all audit staff. This applies equally to research papers and other relevant material.

3. The training co-ordinator Appointing a training co-ordinator is a positive way of promoting various training programmes, particularly where the co-ordinator can undertake some of the actual training. All larger internal audit departments should designate an audit manager as having responsibility for staff training. If this responsibility is extended to cover auditors' career development in line with a suitable programme of individual SWOT analysis then one is well on the way towards quality training. In fact, it is a good idea to make one audit manager responsible

for implementing all human resource management policies and procedures. Where this manager is able to carry out in-house skills training personally, great progress may be made with audit training. Whatever the adopted format, it is clearly essential that all training is properly co-ordinated, or one might fall into the trap of staff attending a variety of courses with the sole objective of making themselves more marketable so that they might leave the organization for a better paid job. The other problem is where training has no relevance to the audit work being performed and is not being applied once learnt. The final drawback in not resourcing a training co-ordinator is that this might lead to a low pass rate for professional exams because insufficient support is made available.

4. Directed reading This is one way of encouraging auditors to research aspects of internal audit. The department should subscribe to all relevant journals and publications. It is possible to assign specific topics to auditors so that each member of the department will research designated audit topics via the world wide web as a contribution to the audit information database. The auditor responsible for (as an example) 'systems interrogation' will research any articles or material that impact on this subject. This falls under 'training' since it involves the assimilation of new information.

5. Training through work Programmed audits enable audit management to ensure auditors are rotated and exposed to a variety of audits and experiences. It is possible to designate smaller audits as 'training audits' where they form part of the auditors' personal development programme. This applies to all audits to an extent. For a training audit, additional budgeted hours will be assigned and extra assistance made available. This is the best type of on-the-job training so long as high standards have been adopted, supervision is good and monitoring and feedback are properly used.

6. The audit review The audit review process enables audit managers and team leaders to direct the work of junior staff and also provides experience in staff management. The process should form part of the training programme by building in the concept of staff development. As such, we are not looking for errors and/or poor performance, but merely providing advice to junior staff on how they might comply with the requirements of auditing standards. This allows a positive interface between audit management and more junior staff and should be seen as such. The review process also provides some training in management techniques primarily based around communication skills where the audit work that has been performed is considered and discussed. A good manager will use the review as an opportunity to provide vital on-the-job training. While being wholly relevant to the task in hand, it should also make reference to best audit practice and the underlying principles. This obviously depends on the presence of 'good' audit managers.

7. Professional affiliations These can be part of CPD and stimulate group discussions. Membership of professional working groups should be encouraged as another way of keeping up to date. Seminars, meetings and presentations all contribute to bringing new thinking into the audit department as long as participants provide feedback once they return to work.

8. The audit manual This sets out the defined methods and procedures required to discharge the audit mission. To feed into the auditor's personal development, this should be assimilated with accompanying skills workshops and training programmes. It is possible to compile a training manual that represents a basic minimum level of expertise required across the department. The

manual defines how these skills will be applied. The audit manual has a wider role in addressing human resource policies on audit training and links into individual career development. The manual should cover:

- The type of training that is available.
- The link into career development.
- The link into performance appraisal.
- How the training needs analysis is carried out.
- How the training budget is managed and controlled.
- The rules on sponsorship for particular courses.
- The rules covering official time off for training.
- How the audit department interfaces with local colleges and other local training organizations.
- A policy on qualifications and whether they are mandatory for specified audit posts.

It may be possible to incorporate all training and development programmes and ideas into an internal audit learning resource where the CAE ensures the following processes are implemented:

- Assign an audit manager with key responsibilities.
- Consider the type of audit resource currently employed.
- Create a vision of the 'new look' internal auditor – define staff competencies to suit (CFIA may be helpful here). It may be possible to divide the audit team into trainees, auditors and senior auditors to assess the degree to which they should demonstrate set competencies.
- Develop policies on moving staff forward – hold a staff workshop to discuss and agree these policies so that they may be accepted, understood, systematic, fair and transparent.
- Talk to stakeholders such as the audit committee and management executive.
- Design a staff development strategy to make the vision real.
- Assign a budget that can be used to implement the strategy. Make sure the benefits outweigh the costs before it goes ahead.
- Identify various development methods and techniques based on training, coaching, education, web-based resources, study groups, quality review, supervision, reading, Internet research, in-house events and so on to use to make the strategy work.
- Assess the existing workforce and design personal development plans based on the performance management system. The position of staff can be assessed through interviews, observation, group discussion, leavers, questionnaires, performance management, procedures, job description, personal experiences and the staff members' and their manager's views.
- Design automated support to work out how best to deliver the material to staff, perhaps through e-learning and interactive development.
- Create measurements to assess how well the process is working (based on planned and actual realized benefits, ideally real on-the-job improvement).
- Remember that learning is the process of acquiring knowledge and understanding, and the learner has to be motivated and able to practise new skills and approaches for learning to work. There must also be a chance to practise and make mistakes before making progress and a barrier to learning is fear of failure.
- Report back to stakeholders on the success or otherwise of the programme.

The Role of the Institute of Internal Auditors

The IIA has a major role in training and development:

Professional examinations These ensure the student has covered a defined series of subjects, and has shown competence in relevant examinations. Some pass without understanding the subject while experienced and capable auditors may perform badly in the circumstances of the examinations hall. A factor is the amount of time one is able to devote to professional studies. A cynic might argue that staff who concentrate on their studies as opposed to their audits may succeed if exam results are the principal performance indicators. Others may prioritize their audit work and fail their examinations. However, employing qualified audit staff (or trainees) is the only way to promote professionalism.

Conferences The IIA organizes seminars and conferences. This provides an avenue for meeting people in the auditing arena and allows open exchange of views.

Periodicals We may subscribe to all relevant periodicals that contribute to the audit database of relevant information. These may include statistical services or other indicators that have a bearing on the organization's particular industry although it does depend on having a procedure for assimilating this new information into the audit database.

Research publications The IIA publishes specialist research papers that may be used by the CAE to develop audit practice. These range from computer audit material through to marketing surveys, which add to the level of knowledge accumulated over the years by the audit department.

District societies The IIA.UK&Ireland is organized geographically into district societies with each member being located in one. They meet regularly and organize events and seminars that may be used in developing the audit function. Keeping up with fellow members in different audit departments can help measure the degree to which they are in line with these trends. Open exchange of views is useful in the search for excellence that forms the cornerstone of the CAE's efforts.

Committee meetings A more proactive approach is applied where one is actively involved in the various committees and working groups that help shape the overall direction of the profession of internal auditing. This not only ensures that one is up to date with current developments but also allows an input into the actual development process itself so that one is not a mere bystander.

Journals and articles Up-to-date and precise articles breathe life into the audit arena and can act as a real-life translation of audit theory. We may keep up with topical debates by reading the latest articles from the IIA journal. It is also possible to build a library covering many specialist areas by using current articles as one very useful source of new material. Technical updates are vitally important to audit management as they may impact on the current audit strategy.

Monitoring Training

Training may be funded and implemented but often there is little follow-up and benefits are not secured. Training not assimilated into the audit role has no benefit and management is responsible for monitoring the effects of training. Available monitoring techniques are

Examination results with a good pass rate This is an interesting indicator in that good results are a sign of a progressive department that is able to produce qualified staff. However, this has to be used with care as there are good audit staff who are not able to master the examination system. Having said this, exam passes are prima facie evidence that the people in

question have reached a defined standard of technical competence. As such, they should make a positive contribution to the audit function. It is important to find out where an auditor has gone wrong where performance in the examinations is poor. It is wrong simply to leave each auditor to struggle through the exams with no support.

Defined improvements in work performance This in one sense is the ultimate goal of most training. If after organizing a series of training workshops on report writing, one finds that the general quality of audit reports is still poor then it may be argued that the programme was not a success. Mechanisms for measuring the performance of staff should always be employed and built into the policy on staff training. It should be possible to plot the progress of each auditor's training programme by making a direct reference to performance appraisal reports.

Better quality of work Auditors can generally be very productive and well versed in the audit process. Some of the training should be targeted at the quality of audit work in conjunction with a quality programme that seeks to improve the various work products. We must then define ways that quality can be measured as a way of gauging the success of any such training. Checks on a sample of audits may be commissioned by the CAE as part of this process and if quality standards do not improve in line with the training then questions must be asked.

Candidates' views on the success or otherwise of the training It is surprising how much can be learnt simply by asking the participant to describe a training course that they have recently attended. There is some correlation between enjoyment and internalization when it comes to courses, since we are more likely to remember events that were enjoyable as opposed to boring. As such, any feedback of this nature can act as a general guide to the success or otherwise of a training session and whether it should be used again in the future.

Informal reviews by general discussion The extent to which a person has progressed as a result of attending a particular training course may also be assessed by reviewing what has been learnt. This is best done on an informal basis. Where this policy has been clearly laid out one might expect a greater motivation from staff who know that they might be 'tested' on the course contents at a later date. One useful way to promote this technique is to ask the participant to give a short presentation of the main points on returning to the office, for the benefit of the rest of the staff. It is also possible to ask the individual to draft a short note for the audit manual where new material impacts on the existing policies and procedures that are applied in the department.

Peer reviews that assess the audit service If there is a shortage of formal training in an audit department this will be commented on in any external review of the audit function. Accordingly, we should expect any training that is carried out to have a positive impact such as to affect the results of any subsequent external review where additional training has been provided. The position on auditor competence with each review will help to establish whether the trend is towards improvements on this front. This in turn will provide an indication of whether training has in fact led to any noticeable improvement so long as these reviews are carried out regularly.

Weekly reviews on progress on quality matters Suitable performance indicators can be used to monitor progress on quality targets. A weekly review of these pointers can help determine whether training is having the desired impact. An increase in training should therefore be accompanied by a corresponding increase in achieving quality targets. This may include meeting audit time budgets, sending out draft reports quickly, restricting the time on non-recoverable work and so on.

Client feedback on the quality of the audits that have been recently carried out Quality assurance procedures require that the client provides feedback on whether audit objectives have been achieved. The information that may be gleaned from a suitable questionnaire sent to audit clients can be used to assess the efficiency and effectiveness of auditors and isolate any particular trends. Any training needs relating to, say, communications skills will be quickly identified via this technique and one may direct training towards this area or discover whether relevant past training has been effective.

Increase in the overall level of auditors' morale This is a more general indicator that is based on the premise that staff who are well trained and developed are more motivated and content than staff who have been ignored in this respect. This need not be overly scientific as one may sense very quickly whether there is constant complaining about the lack of support from management, where this is the case. On the other hand, an atmosphere where staff are eager to discuss the latest technical developments does indicate a positive culture and can also be readily identified.

The Link into Development

Training is part of the managerial process and as such forms only one constituent of the overall system of human resource management. It cannot be seen in isolation from the other techniques for developing audit staff. Training must be set clearly within a formal auditor-development programme that tracks the progress of each auditor throughout their career with the organization. There are several relevant points that may be made in this respect:

- Each auditor should have a personal development programme that is carefully reviewed and monitored, particularly in terms of training needs.
- The development programme should be linked to a formal performance appraisal system that seeks to set standards and judge whether these are being achieved.
- Audit training must be linked into this programme as one way of closing any skills gaps that have been identified via the above mechanisms.
- The development programme should also be capable of reviewing the extent to which training has improved the auditor's performance.
- The training co-ordinator, whose role was mentioned earlier, should ideally have a wider function in monitoring each auditor's personal development programme.

The 'short-stay syndrome' results because organizations view internal audit as an ideal place to train managers. There are many who do not view internal audit as a career in its own right and, for example, trainee accountants may wish to return to main-line accountancy after a spell in audit. This poses a problem in that extensive training is lost on audit staff who will not remain with the department for long. All staff should be developed and those who may wish eventually to leave auditing will simply be replaced by other auditors. Vacancies create scope for internal promotions for auditors who excel via their development programmes. The only concern is that short-stay staff should not be placed on professional qualification programmes as these last several years and require a major commitment to a career in internal auditing.

Building on Existing Knowledge

Training is a developing process with no natural start and finish. The auditor should build on existing skills and knowledge to achieve higher levels as they acquire increasing degrees of expertise. This model of audit training can be illustrated diagrammatically in Figure 5.16.

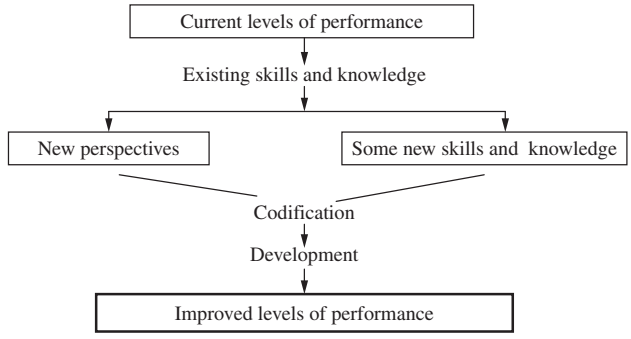


FIGURE 5.16 Building on existing skills.

The idea is to direct training at skill areas that the auditor is familiar with and uses in day-to-day work. Training consists of setting a clear perspective within which existing skills and knowledge may be reappraised by the auditor. An ongoing process of codifying these skills so that they may be better directed at the achievement of audit objectives is established as a key role for the trainer, while new knowledge may also be imparted. The secret is not to try to teach new skills, but to build on existing skills and develop a sensible framework within which they may be better applied. This recognizes how difficult it is to teach new knowledge that has no base to which it may attach itself. It acknowledges the need to link training into real-life experiences. Remember that it has been said that all theories are wrong, but some can nonetheless be useful. The Handbook seeks to set a conceptual framework that will be translated by auditors according to their work environment. Training costs money and must be properly managed. This means developing individual auditor-training profiles and linking this to a developmental programme. It must be co-ordinated and carefully monitored and, ideally, integrated into a formal quality assurance programme. Training must not only be funded and applied, it must also be managed and controlled as part of wider human resources management that should underpin resourcing the audit function. A simple tool may be used to assess the training and development strategy in use, by considering a set of basic benchmark questions in Table 5.5.

5.11 New Developments

The Institute in the UK and Ireland believes that Internal Audit communications are most valuable when they include a clear conclusion and opinion related to the objectives and scope of the engagement:

> This is the end result of careful planning, gathering of evidence and thoughtful evaluation. Internal audit communications have their value in providing assurance that risks are being managed effectively and in catalysing and facilitating improvements where appropriate. The form and content of communications vary widely; there is no right or wrong way to prepare an internal audit report. What is important as indicated in the International Standards and Practice Advisories is that reports, spoken or written, should firstly contain sufficient, relevant and useful information to provide a sound basis for conclusions and opinions. Secondly, the communication is most valuable if contains the internal auditor's conclusion and opinion on the adequacy and effectiveness of the relevant processes and the need for improvement where appropriate. This approach will enable the internal audit department to express an overall view upon whether the organisation's system of internal control is effective in managing its risks within its risk appetite.[28]

TABLE 5.5 Analysing your audit training strategy.

A. Key control – vision: To ensure top audit management has a clear vision of (and commitment to) the role of training and development. (Risks – No real support from CIA means the initiative will fail.)	Yes	No
A.1 Does the CAE set clear targets for training and development (T&D)?		
A.2 Is T&D seen as a key component of success in term of targets of service excellence?		
A.3 Do your staff recognize and support the need to respond to the growing expectations from top management?		
A.4 Is T&D a regular agenda item at audit management meetings that is action oriented?		
A.5 Do the CAE and audit managers reserve time for their own personal development?		
A.6 Is there time set aside for regular in-house training seminars?		
A.7 Do you accept the principle that you cannot afford NOT to develop your staff?		
A.8 Are you able to 'Go Fishing' and trust your staff to take care of business?		

B. Key control – learning culture: To ensure the work environment actively promotes the continuous development of employees. (Risks – T&D will have little impact without an underlying learning culture.)	Yes	No
B.1 Have you defined a formal set of audit competencies for: junior auditors, senior auditors and audit management?		
B.2 Does your audit manual set high standards for audit work and reflect an up-to-date position of audit products and processes?		
B.3 Do you use the audit review process to develop your auditors and isolate training needs?		
B.4 Do audit managers and staff constantly seek new ideas and experiences from external sources which are fed into the risk-based audit strategy?		
B.5 Do more senior and experienced staff leave room for 'Capacity to Learn' in their mindsets?		
B.6 Does your audit shop accept that the rate of learning must be greater than or equal to the rate of organizational change?		
B.7 Have you interfaced the research on audit competency (CFIA) into recruitment, promotion, appraisal and T&D strategies?		
B.8 Have you considered the competence-based NVQ scheme for some of your internal auditors?		
B.9 Do your T&D policies recognize that studying for and passing exams does not necessarily equip staff with the skills needed to perform well?		
B.10 Are you in a position to implement the competence-based approach for training and developing your auditors?		

C. Key control – resources: To ensure the required continuous development activity is properly resourced and budgeted for. (Risks – Good intentions will have little impact without the resource implications established and committed.)	Yes	No
C.1 Do you have an audit manager who is designated audit training co-ordinator?		
C.2 Do you have auditors who are competent in training needs analysis, training course design and presentation skills?		

TABLE 5.5 (*continued*).

C.3 Do your audit supervisors have time for a *coaching*, style where juniors are encouraged to solve any problems encountered in the audit?		
C.4 Do you seek advice from Human Resources on training needs, strategies and budgets?		
C.5 When you use an external trainer, do your senior staff work closely with this person so that they might run the training event in future?		
C.6 Is time set aside for continuous T&D activities that are recognized in job budgets?		
C.7 Do you have a training budget that reflects the need to prioritize this aspect of staff management?		
C.8 Do you make good use of corporate T&D budgets, programmes and facilities?		
C.9 Do you have access to a quality training room that is equipped with suitable facilities for successful in-house training events?		
C.10 Do you invest in CDs, publications, journals (and time for Internet enquiries) to promote continuing research and development?		

D. Key control—process: To ensure there is a clear and workable process for supporting the continuous development of employees. (Risks—T&D will have little impact if not supported by formal procedures and programmes.)	Yes	No
D.1 Have you developed a formal audit T&D strategy which is derived from your organizational strategy?		
D.2 Is your audit T&D strategy designed to develop highly skilled auditors and tackle all defined weaknesses in your current staff?		
D.3 Does your performance appraisal system help you isolate training gaps and is it interfaced with your training strategy?		
D.4 Does each auditor have a documented personal development plan that involves exposure to different aspects of audit work?		
D.5 Do you hold in-house workshops: at least once a month on new developments with defined learning goals, which are then evaluated?		
D.6 Do you hold formal induction training for new starters based on your audit standards (from your audit manual)?		
D.7 After the audit staff have attended an external training event do you get them to do a presentation on what was learnt and any impact this new information may have on the current audit strategy?		
D.8 Does your training and development strategy help your organization meet its overall mission in life?		
D.9 Are staff encouraged to get together spontaneously and 'Flip Chart' through a specific problem?		
D.10 Are all T&D activities put together in a staff development portfolio geared at cost-effective development initiatives?		

Developed by Spencer Pickett ©1999

One important development is found in the exact role of the CAE and the range of responsibilities they assume. In some organizations, this role has expanded to become chief risk officer and even covers the whole range of responsibilities that fall under the concept of governance, risk and compliance. This has major ramifications for the profession of internal auditing as we decide how much more to take on as part of the audit role or as a separate addition to the main internal auditing duties. Being in charge of the quality of the risk management process, even if it is owned

by management may make it difficult to audit this same process for the audit committee. Perhaps the CAE can act as co-ordinator and ensure that risk decisions are made by the appropriate head of business lines and that there is a risk committee to oversee the arrangements. But to retain objectivity, the CAE would need to be careful about assuming responsibility for activities that fall outside the range of internal auditing. But if internal audit were responsibile for all assurance activities, then a fully integrated position may be prepared and reported to the board. If the board were to require an external review of the CAE's empire, then governance, quality and possible conflicts pertaining to independence could be assessed and dealt with. The key is to ensure business managers are fully responsible for risk management, compliance and control in their areas of responsibility. Internal audit will then provide assurances on risk management, controls, fraud, compliance and governance arrangements, and not be responsible for these concerns, simply responsible for reviewing their effectiveness. Sound advice on the role of Internal Auditing in governance has been provided by the OECD in their Principles of Corporate Governance:

> Internal auditing typically operates in two capacities. First, auditors provide independent, objective assessments on the appropriateness of the organization's governance structure and the operating effectiveness of specific governance activities. Second, they act as catalysts for change, advising or advocating improvements to enhance the organization's governance structure and practices. In an organization, management and the board establish and monitor companywide systems for effective governance. Internal auditors can support and improve these actions. In addition, although internal auditors should remain independent, they may participate in the establishment of governance processes. By providing assurance on the organization's risk management, control, and governance processes, internal auditing becomes a key cornerstone for effective organizational governance. Which capacity is most relevant for internal auditing is highly influenced by the maturity level of the organization's governance processes and structure, and the organizational role and qualification of internal auditors. In an organization with a less mature governance structure and process, the internal audit function may be focused more on advice regarding optimal structure and practices, as well as comparing the current governance structure and practices against regulations and other compliance requirements.[29]

The experts in the field, the IIA, have given their views on the expending role of internal auditing in organizational governance:

> Internal auditing will often be most effective in dealing with governance activities by doing more than performing discrete audits of specific processes. An internal auditor's unique position in an organization allows him or her to observe governance structure and design, while not having direct responsibility for them. Often, internal auditors can assist organizations better by advising the board of directors and executive management on needed improvements and changes in structure and design, not just whether established processes are operating. This is different, however, from providing objective assessment of specific governance activities through discrete audits. Ultimately, internal audit assessments regarding governance activities are likely to be based on information obtained from numerous audit assignments over a period of time. Optimally, internal auditors should aim to provide assessments on the effectiveness of key organizational governance elements, either separately from, or combined with, assessments on the effectiveness of risk management and key controls. These governance activity assessments should take into account:
>
> - Provide advice that focuses on the organization's governance structure to meet compliance requirements and addresses basic organization risks.
> - Perform audits of design and effectiveness of specific governance-related processes.

- Evaluate best practices and their adaptation to the organization by focusing on the optimization of governance practices and structure.
- Allocation of Audit Effort.
- Less Structured More Structured.
- Specific governance assignments.
- The results of specific board-level governance review work.
- Governance issues arising out of myriad audit assignments performed during a specific period of time.
- Other information available to or known by the internal auditor.

> Internal auditors may operate most effectively for the board as an agent of the board who provide independent, objective information and evaluation. The board would then own internal auditing, fostering a mutually supportive internal audit-board relationship. To gain a complete understanding of the organization's operations, it is essential that the board consider the internal auditor's work. For instance, internal auditors can inform the board on matters such as culture, tone, ethics, transparency, and internal interactions. In addition, contemporary internal auditing is based on the organization's framework for identifying, responding to, and managing the different strategic, operational, financial, and compliance risks facing the organization. As a result, internal auditors can provide objective assurance on the effectiveness of the framework as a whole, including management's monitoring and assurance activities, and on management of individual key risks. This role of supporting the board, however, can create tensions because internal auditing also may be positioned as a partner to management. Internal auditors will need to manage the needs and expectations of both constituents carefully.[30]

While in their blueprint for the internal audit profession, the IIA suggest that internal audit functions should undertake four main tasks:

1. Work more closely with senior management to ensure the key risks to their organization are identified.
2. Identify skills gaps which stop them providing assurance over key risks and work with management to plug those gaps.
3. Take care that they move into new areas only if they can agree with management that this will be valuable in providing assurance over key risks and if they are confident they have the required skills.
4. Co-ordinate assurance activities over these key risks.[31]

There are calls from around the world to make internal audit mandatory in all publicly quoted companies, or ensure that there is careful consideration for setting up such a team. The International Corporate Governance Network (ICGN) has added its voice to the debate in their global corporate governance principles:

> Companies should establish and maintain an effective internal audit function that has the respect, confidence and co-operation of both the board and management. Where the board decides not to establish such a function, full reasons for this should be disclosed in the annual report, as well as an explanation of how adequate assurance has been maintained in its absence. The internal audit function should have a functional reporting line to the audit committee chair. The audit committee should be ultimately responsible for the appointment, performance assessment and dismissal of the head of internal audit or outsourced internal audit provider. The external auditor should not provide internal audit services to the company.[32]

Internal audit's role in the risk management agenda has been given a boost by the IIA in their significant guidance covering ten Risk Management Imperatives that Internal Auditor's should be considering:

1. Assess the Organization' Current Processes and Capabilities

To strengthen organizational risk management, internal auditing should first conduct a detailed assessment of the organization's risk management processes, many of which might be undocumented and informal. The assessment should help build an inventory of risk processes and serve as a foundational baseline. It should also help determine the organization's ability to identify, analyze, monitor, and mitigate significant risks that could impede achievement of organizational objectives.

2. Co-ordinate With Other Risk and Control Functions

Look for opportunities to partner with other risk and control functions while maintaining your functional independence and objectivity. For example, consider involving other risk and control functions in the assessment of risk management processes recommended in Imperative No. 1. Also consider how the functions can collaborate on an enterprisewide assessment of risk management processes. Roundtable participants agreed that most organizations would benefit from a common, single risk assessment developed by internal auditing in concert with other governance, risk, and control (GRC) functions in addition to a single risk profile. It's also important to establish communication protocols and procedures to share risk knowledge and information on an enterprisewide basis.

3. Participate in Summits With Key Stakeholders

To many observers, risk oversight is the No. 1 priority for directors and management alike in today's post-meltdown business environment. It's critical for CAEs to facilitate in-depth discussions with senior management and directors about risk management issues and priorities to ensure that internal auditing and other key risk players understand their chief stakeholders' expectations. Ideally, such an effort would be conducted jointly by internal auditing and any other key risk and control players, such as the chief risk officer, in addition to senior financial officers. Plan to brief members of the audit committee and senior management on a regular basis and consider holding a series of educational seminars with directors to provide an ongoing vehicle for two-way communication on this essential topic.

4. Help the Organization Develop Near-term Strategies

After assessing current risk management processes, and revisiting stakeholder expectations, try to facilitate the development of near-term organizational risk management strategies. Discussions at the roundtable point to the benefits of organizations taking a step-by-step approach to risk management. Accordingly, facilitate a plan to achieve the organization's next step in terms of risk management maturity as opposed to the final stage in the developmental process. Although internal auditing should refrain from any decision-making role in the development of risk management strategies, the CAE can serve as a valuable adviser to both senior management and the board of directors. If your organization lacks an ERM strategy, suggest options for consideration. Scope out the benefits of a step-by-step approach to ERM and suggest what these steps might be. Also consider delineating the roles of the various risk and control functions relative to risk management.

5. Strengthen Top-level Communications

As the organization steps up its focus on risk management, keep executive management and the audit committee well-informed of the organization's progress and strategic direction. Explore how to enhance risk reporting to the committee and seek to make risk considerations a central discussion item on the audit committee's agenda.

6. Define Internal Auditing's Role

After facilitating a strategic reassessment of the organization's approach to risk, work with chief stakeholders to develop an appropriate role and strategy for internal auditing related to risk management. If the organization's risk management processes are in the developmental stage, internal auditing might prefer to adopt a consulting role. Conversely, if risk management processes are developed sufficiently to audit, then internal auditing can play an assurance role. Practitioners should recognize that internal auditing's role will likely evolve along with the organization's risk management processes.

7. Audit Risk Management Incrementally

Roundtable CAEs spoke enthusiastically about the benefits of taking a step-by-step approach to auditing risk management. "You can't audit all of your company's ERM activities but you can evaluate parts of them and look at how they get their data," said one CAE. "Bite off manageable chunks; audit risks in a given area," said another. "Don't try to be world-class all at once," said a third CAE. When it comes to setting priorities, audit committees and executive management want internal auditing to concentrate on areas posing the greatest risks – those that could impact achievement of major corporate objectives. Make sure to identify and monitor key strategic, operational, and business risks, advised one roundtable CAE. Another recommended singling out the three to five risks that could destroy the organization, including the types of high-impact, low-probability risks that contributed to the subprime mortgage crisis.

8. Assess Audit Skills and Capabilities

One of the challenges facing internal auditors seeking to expand their scope of risk management activities is the perception that risk management is beyond the scope and capabilities of internal auditing. "Many auditors think control first and lack an adequate business perspective," said one roundtable CAE. "Internal auditing needs to provide value beyond compliance, and it's hard to add value when you've been focusing on Sarbanes-Oxley," said another.

9. Execute the Audit Strategy With Appropriate Reporting

Effective reporting is central to successful internal auditing and risk management. Determine the type of reporting that best suits your particular internal audit function. For organizations with more formal or maturing risk management processes, it might be appropriate to perform audits and then issue assurance reports. For organizations that are just developing risk processes, internal auditing might play a more consultative role and issue consulting reports. If the organization has yet to produce any risk reports, internal auditing should consider other types of reporting that could provide management and directors with important updates on the organization's risk profile or other risk-related changes. Auditors should also consider providing the audit committee with periodic updates on the implementation of management's risk management strategy.

10. Keep up With Evolving Practices

As risk management practices and processes continue to evolve, it's important for CAEs to keep abreast of relevant internal audit practices and to ensure the organization benefits from their up-to-date insights and perspectives. For example, credit rating agency Standard & Poor's has begun to include ERM assessments in its ratings of non-financial companies (see page 16). In addition, the National Association of Corporate Directors, The Committee of Sponsoring Organizations of the Treadway Commission, and other leading organizations are producing numerous studies and papers focusing on risk management practices that offer useful information and insights for internal auditors.[33]

Risk imperative two is interesting as it calls for building bridges with other risk and control functions. This idea takes us further into our discussion of the respective responsibilities of the

CAE and the chief risk officer. It is a question of time before the committee or the risk committee calls for the integration of the risk and control functions along with an integrated approach to reviewing and reporting back the assurances arising from these teams. The call for enterprisewide risk management, enterprisewide risk reporting and the same approach to the assurance process means organizations may be able to simplify the way risk is managed and reviewed by everyone within the organization.

There is no escaping the fall-out from scandals such as Enron, WorldCom and Xerox and the IIA – UK and Ireland (IIA) has issued guidance in the wake of these high-impact corporate financial scandals that impact the internal audit role:

> The key lessons to be learned from the recent corporate scandals are centred on a better understanding of the need to realise the value of effective corporate governance.
>
> - The role of the board must in future be significantly enhanced. Each board member needs to understand clearly their duties and obligations. There must be a better framework for the board to interact with other parties that have responsibility for independent assurance, such as internal audit and the audit committee. The effectiveness of the board must also be enhanced through an increased and better informed level of participation by non-executive directors. The board must have available to it all forms of reliable information to be in a position to properly understand the real business risks facing the organisation and to explore issues in sufficient depth. This requires that the board must commit sufficient time on a regular basis for meetings.
> - The internal audit function must have the professionalism, profile and independence to fulfil its role effectively. It must be able to provide an environment of challenge, transparency and candid reporting to the highest level without fear and retribution. Internal audit must provide the focus on risk for the organisation. It must demonstrate a good understanding of the organisation's business operations together with communication and persuasion skills to get its message across. The IIA's international Standards are the benchmark against which effective internal audit functions can be measured.
> - Loyalty to the right stakeholders and serving the right interests. Executive management serve the organisation and exist to preserve and protect it from exposures to risks of any kind. Internal auditors provide independent assurance to executive management and the board about the adequacy and effectiveness of the risk management and control framework in operation and seek to improve that framework through the promulgation of best practice. Both parties should also be aware of all stakeholder interests in the organisation. External auditors serve the interests of the shareholders and investors in the company. Alarm bells should ring when there is a perceived shift in loyalties and priorities.[34]

The scandals continue with the 2007–08 Credit Crunch where internal audit is being asked to redefine its role as the world calls out for more control over reckless behaviour from businesses that fail to recognize the systemic risk that comes with global trading.

Summary and Conclusions

The challenge has been set by the corporate governance, risk management and control dimensions that now drive both the business world and public services. The definition of internal auditing has been changed to reflect this factor, and audit charters are being torn up and rewritten to secure this important focus. Everything else that happens in internal audit flows from the changes, charter

and heightened expectations. We can summarize this development by using a simple model in Figure 5.17.

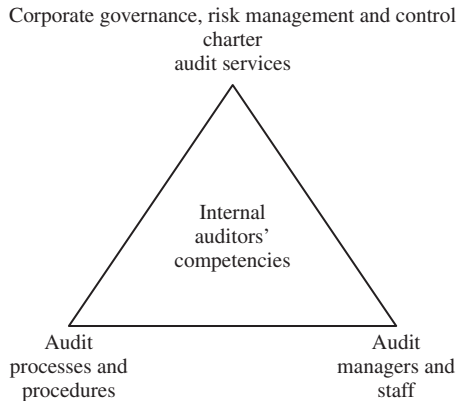


FIGURE 5.17 Internal auditing competencies.

We have already mentioned the corporate governance, risk management and control context of internal auditing. This is incorporated into the audit charter and in turn determines which audit services are provided. The second part of the triangle is the audit processes and procedures, that is the way audit work is performed to provide risk-based assurance and consulting services. The third dimension is the people who are recruited and retained at audit manager level and below, to perform the actual services (using the set procedures). Internal audit competencies sit in the middle of the triangle as the key to ensuring the rest is achieved. So long as we have the right people doing the right things to set standards there is a good chance of success. If there is no focus on developing competencies to reflect the new expectations, then there is no real starting place for tackling the 'raised bar'. Raising the bar for the internal audit shop has been a key consideration for many standard setters and one such proponent is Natwest Audit who have explained how they set new standards:

> The Financial Services industry and the markets we operate in are becoming more complex and competitive. To meet these challenges, businesses within the Natwest Group have to adapt, improve and innovate. Striving for competitive edge is constant. At Natwest we decided that this created an excellent opportunity to really rethink how our internal audit function can make a contribution to a business. We decided to embark, with full stakeholder support, on a journey to a richly imagined future. To create an internal audit function which rewrites the standards for adding value to the Group, its businesses, and to our people. The first thing that changed was our mandate which redefined our role and purpose. Reflecting the needs of the Board and other stakeholders, we are mandated to provide:
>
> - Assurance that the current risks in our businesses are being managed adequately and in a cost effective manner and to have the courage to state where such assurance cannot be given.
> - Assurance that the risks surrounding the development of our future organization are being managed and that our future businesses will contain effective and efficient controls from day 1.
> - Solid respected judgements to guide and influence management action.
> - Continuous expert advice to provide stimulus for the business to continuously improve.

> So what needed to change? Well, almost everything: new organizational structure, new skills sets, new processes, new technology, and new way of working and, at the heart of it, a new way of thinking.[35]

All audit shops should be thinking about the way they raise the bar and ensure they do not stumble at the first attempt.

Chapter 5: Assignment Questions

Having worked through the chapter, the following questions may be attempted (see Appendix A). Note that the question number relates to the section of the chapter that contains the relevant material.

1. Provide a commentary on the issues raised in the paper on 'Dialectics and Internal Audit,' and how this work contributes to the development of the audit perspective.
2. Discuss the definition of internal auditing and how the wide scope of work represents a challenge for the internal auditor.
3. Explain the importance of an up-to-date audit charter and comment on the items that will feature in the charter.
4. List the types of services provided by internal audit shops and comment on the implications of the wide variety of these services.
5. Explain why independence is important to the internal auditor and discuss the issues that should be considered in ensuring internal audit is sufficiently independent.
6. Discuss the need for a suitable code of ethics for the internal auditor and describe some of the items that should form part of such a code.
7. Explain the need for good working relationships between the internal auditor and the client and discuss why there may be problems with differing expectations, and suggest how these problems may be overcome.
8. List and describe some of the matters that may fall under the guise 'frequently asked questions' from users of the internal audit website.
9. Explain what makes a good auditor in terms of competencies, and describe what the CAE may do to ensure these competencies are developed and maintained.
10. Prepare a presentation to the internal audit management team on the way an audit training strategy and programme may be developed and implemented.

Chapter 5: Multi-Choice Questions

5.1 Which is the most appropriate statement?
   a. Internal audit is a nearly full-blown profession. This means it has a clear set of professional standards and is able to work to best practice guidelines in delivering a quality service.
   b. Internal audit is now a full-blown profession. This means it has a clear set of professional standards and is able to work to best practice guidelines in delivering a quality service.
   c. Internal audit is now a full-blown profession. This means it has a clear set of professional standards and is able to work to best practice guidelines in delivering an okay service.
   d. Internal audit is now a full-blown profession. This means it has a clear set of professional standards and is able to work to best practice legislation in delivering a quality service.

5.2 Insert the missing words:
   The charter formally documents the ..... of the audit function
   a. raison d'être

b. expectations
c. desires
d. independence

5.3 Which is the odd one out?
The audit charter establishes audit's position within the organization and will address several issues:
a. The nature of internal auditing
b. The audit objectives
c. The scope of audit work
d. The staffing levels
e. Audit's responsibilities
f. Audit's authority
g. Outline of independence

5.4 Which four of the following statements are inappropriate?
a. The charter should be simple and short, preferably contained within a single sheet of paper that will fit on a web site screen.
b. The concept of audit independence should be highlighted.
c. If senior management in the organization does not support the charter then considerable problems will ensue.
d. The reporting process should be briefly described.
e. The auditors' code of ethics should be documented in the charter.
f. The requirement that internal audit assume no line responsibilities in the organization should be noted.
g. The position regarding responsibilities for detecting, investigating and resolving frauds should be clearly established.
h. A note regarding the need for full co-operation with the organization's external auditor may also be included.
i. The charter should be a statement of basic principles and not a procedures manual.
j. The charter should be formally approved by the DF.
k. A poorly thought-out charter (or for that matter, where there is no formal charter in existence) has a knock-on effect on other standards that are really dependent on the formal authority to discharge an audit service.
l. As noted, unrestricted access cannot be agreed within the charter and this should be negotiated at all levels throughout the organization.
m. The charter should be a standing document and should not require changing for many years.
n. The scope of audit work should include non-audit consultancy work as a direct response to meeting management's needs.
o. Whatever the expectations implied by the charter, the CAE should ensure that the audit function can meet them.

5.5 Insert the missing words:
Internal audit shops that focus on the ....., rather than take on any work that comes its way, will tend to have a better direction.
a. control compliance arrangements
b. management referrals
c. financial reporting systems
d. corporate governance arrangements

5.6 Insert the missing words:
The ..... can be used as a framework for developing appropriate audit services. The question to ask is: how can we best contribute to risk management, control and governance services, through both our assurance and consulting roles? The answer will help define
a. audit committee
b. IIA definition of internal audit
c. audit staff competencies
d. audit manual

5.7 What is abc?
All definitions of internal audit contain the word 'abc' and this is an important component of the audit role. It is both a concept and an ideal. One could assume that since internal audit is located within the organization it cannot be abc.
a. outstanding
b. reliable
c. flexible
d. independent

5.8 Which bullet point is wrong?
There are many positive images that are conjured up by this concept of independence:
a. Objectivity
b. Impartiality
c. Unbiased views
d. Valid opinion
e. No spying for management
f. Not many 'no-go' areas
g. Sensitive areas audited
h. Senior management audited
i. No backing-off

5.9 Which of the following statements is most appropriate?
a. Where internal audit reports to the FD, this enhances the status of the audit process and promotes good audit work.
b. Where internal audit reports to the FD, a careful approach has to be negotiated to secure the degree of independence that promotes good audit work.
c. Where internal audit reports to the FD, all reports should be copied to the audit committee to secure the degree of independence that promotes good audit work.
d. Where internal audit reports to the FD, there is great scope to achieve the independence to promote good audit work.

5.10 Which of the following statements is most appropriate?
a. The policy of talking to management and incorporating their needs into the project terms of reference creates a positive process but may be manipulated to lessen the level of independence. One would accommodate management's views but only to an extent, so as not to alter the original terms of reference beyond recognition.
b. The policy of talking to management and incorporating their needs into the project terms of reference creates a negative process that may be manipulated to lessen the level of independence. One should not accommodate management's views if this would alter the original terms of reference.
c. The policy of talking to management and incorporating their needs into the project terms of reference creates a negative process but may be manipulated to lessen the level of

independence. One would accommodate management's views but only to a very limited extent.

d. The policy of talking to management and incorporating their needs into the project terms of reference creates a positive process that increases the level of independence. One would always accommodate management's views to ensure the project has a terms or reference that is set by management.

5.11 Insert the missing words:

Courtemanche discusses four styles of auditing that are akin to adopted audit philosophies:

a. The .....: The auditor represents an outside interest with a regulatory role in the organization. (one word)

b. The .....: The audit role is as an agent for senior management and a special status is therefore acquired. (three words)

c. The .....: This is the worst situation where the auditor is self-answerable and not to management or an outside regulatory agency. (one word)

d. The .....: The auditor distorts the admirable qualities of honesty and integrity to 'tell it like it is'. (one word)

5.12 Which of the following factors is wrong?

The Rittenberg model on audit independence contains several factors:

a. **Organization:** This deals with the position of audit within the organization and covers all relevant factors including reporting levels, top management support, audit committees and the audit charter.

b. **Economic:** These factors relate to the management of the audit department and include policies on designing systems, staffing the audit function, ethics, time restrictions on work and supervisory review.

c. **Remuneration**: Sufficient levels of remuneration should be applied to the audit resource to ensure a professional service.

d. **Mental state:** Factors in this category should ensure that the auditor does not subordinate his/her judgement as required by the standards. The important areas are personal attributes, objectivity, competence and professionalism in providing audit services.

5.13 Insert the missing words:

The CAE should continuously seek out ways to improve the level of objectivity throughout audit and some of the relevant matters have been mentioned earlier. A great deal of this hinges on installing suitable ....., the aim being to remove any potential barriers.

a. staffing arrangements

b. whistleblowing procedures

c. policies and procedures

d. checks of audit work

5.14 Insert the missing words:

The client might wish to have internal audit perform a series of consultancy projects generated by ad hoc problems that they as managers may experience. The professional auditing standards seek to promote audits that involve reviews of control systems as a service to the entire organization as a wider concept. The conflict arises where the problems referred to audit by management result from .....

a. incompetent auditors

b. inadequacies in controls

c. overly demanding problems
d. a lack of resources

5.15 Which of the following statements is most appropriate?

a. Where there is a conflict between consultancy and audit services, then this needs to be handled with care.
b. Where there is a conflict between consultancy and audit services, then the CAE should monitor the projects.
c. Where there is a conflict between consultancy and audit services, then consulting services should reign supreme.
d. Where there is a conflict between consultancy and audit services, then audit services should reign supreme.

5.16 Which of the following statements is most appropriate?

a. Independence must be guarded at all costs and sufficient independence is needed to enable professional audit work to be carried out and acted on by management.
b. Independence cannot be guarded at all costs and only sufficient independence is needed to enable professional audit work to be carried out and acted on by management.
c. Independence cannot be guarded at all costs even though absolute independence is needed to enable professional audit work to be carried out and acted on by management.
d. Independence cannot be guarded at all costs and only sufficient independence is needed to enable professional audit work to be carried out even where it is not acted on by management.

5.17 What is 'xxx'?

A xxx is necessary and appropriate for the profession of internal auditing, founded as it is on the trust placed in its objective assurance about risk, control and governance. The xxx applies to both individuals and entities that provide internal audit services.

a. dedicated audit secretary
b. focused audit report
c. code of ethics
d. audit charter

5.18 Which model is wrong?

The late Gerald Vinten has developed three models of morality:

a. The regulatory model. This approach sees the question of morals as being based on instructions from the appropriate authorities.
b. The compliance model. This model argues that people need to comply with ethical codes.
c. The aspirational model. This model appeals to the higher levels of humanity with the concept of morals seen as something that glows from within.
d. The educational model. This is the most appropriate model where morality is seen as a set of concepts that may be learned.

5.19 Which of the following is wrong?

The alternatives to the word 'Audit' from a standard thesaurus include the following terms:

a. examination
b. scrutiny
c. inspection
d. investigation
e. consultant
f. review

5.20 Insert the missing words:
Auditors should be skilled in dealing with ..... and as such this aspect is seen as a valid audit skill. Unfortunately, this skill does not always form part of the auditors' professional training and development programme. In fact, a poor recruitment policy may result in bringing in auditors who see little value in developing good inter-personal skills
a. problems
b. people
c. risks
d. processes

5.21 Insert the missing words:
Research into the '..... ' shows that formal long-winded audit reports have little impact on busy managers. They want to know in short simple words 'what the problem is, and what they should therefore do about it'.
a. one-minute manager
b. five-minute manager
c. speedy manager
d. fast track manager

5.22 Insert the missing figures regarding attitudes among employees towards internal auditors from the selection below (per Churchill):

ATTITUDE	%
NEGATIVE	
NEUTRAL	
POSITIVE	
MIXED	

a. 02%
b. 24%
c. 26%
d. 48%

5.23 Insert the missing figures regarding perception of who internal auditors were most like (per Churchill):

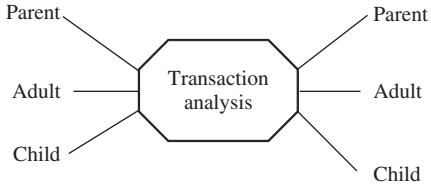
RESEMBLES	%
TEACHER	
POLICEMAN	
ATTORNEY	
MIXED	

a. 08%
b. 11%
c. 23%
d. 58%

5.24 Which of the following suggestions is wrong?
Mints set out a number of ways that auditor/auditee relations might be improved:
a. Better understanding and communications by the auditor.
b. Use a mutual problem-solving, rather than blame assignment approach in line with participative team building.
c. Educate auditees in the usefulness of audits.
d. Ensure management implements all audit recommendations straight away.
e. Obtain management's view of the problem.

5.25 Insert the missing word:

Relationships consist of various transactions:



The most efficient working model is where the .....

a. 'child' communicates with the 'child'.
b. 'child' communicates with the 'adult'.
c. 'child' communicates with the 'parent'.
d. 'parent' communicates with the 'parent'.
e. 'parent' communicates with the 'adult'.
f. 'adult' communicates with the 'adult'.

5.26 Insert the various words into the most appropriate Box of the table:

FACTOR	TRADITIONAL STYLE	PARTICIPATIVE STYLE
ROLE	Box 1	Box 2
AUTHORITY	Box 3	Box 4
SOURCE OF AUTHORITY	Box 5	Box 6
SANCTION	Box 7	Box 8

a. Advisor
b. Coercion
c. Formal
d. Informal
e. Office
f. Personal attributes
g. Policeman
h. Suggestions

5.27 Which of the following statements is inappropriate?

There is great scope in participative auditing and it has several positive features that can be summarized:

a. It involves management in the auditing process as part of the team rather than using audit as a management spy.
b. It is not merely a question of being nice to the client as it has a more dynamic element that involves some flexibility on both sides.
c. It can be more interesting in that it is geared into error discovery and the audit findings are placed into perspective according to a clear prioritization process.
d. It can be more demanding where many complicated issues have to be built into the work and the auditor will have to decide how far to alter draft reports to reflect management's views.
e. The results are discussed and agreed as the audit proceeds with regular interim reports and management may actually assist in developing proposed solutions.
f. Managers are able to share their problems. It is also advisable to review the reports with lower levels of management.

g. It can engender more commitment all round.
h. The auditor is able to address major issues.
i. It promotes good co-operation between audit and management that can be used to build a client base across the organization.

5.28 Insert the missing word:

Client expectations of ..... internal audit services typically consist of:

- A check on remote establishments to ensure that they are complying with procedures.
- The investigation of frauds where they have been detected within the organization.
- Investigations into employees who cause concern to management in terms of breaching procedure.
- A continuous programme of checks over the output from various financial systems to assess whether these are correct.
- On-the-spot advice as to whether proposed management decisions are acceptable in terms of compliance with procedure and best practice.
- Ad hoc investigations requested by members of the corporate management team.
- Additional resources for computer system development projects.

a. futuristic
b. traditional
c. risk-based
d. dynamic

5.29 Insert the missing word:

..... managers may be defined as senior officers who are working to objectives that are inconsistent with organizational objectives.

a. Delinquent
b. Motivated
c. Confused
d. Unaudited

5.30 Which statement is least appropriate?

The benefits of training for internal auditors includes:

a. Increase in the quantity of work done by auditors.
b. Better quality of work.
c. Cost savings in terms of better overall performance.
d. Better standard of report writing.
e. Better quality of working papers.
f. Less audit staff required in the long term.
g. Smaller training gap in terms of skills shortages.
h. More detailed supervision of audit work.
i. Greater degree of professionalism.
j. Better motivated workforce with career development programmes.

5.31 Insert the missing words:

The '..... syndrome' results because organizations view internal audit as an ideal place to train managers.

a. short-stay
b. professional-auditor
c. career auditor
d. long-stay

References

1. Perrin Sarah 'Assurance services'. *Internal Auditing*, July 1999, p. 6.
2. Chambers Andrew and Rand Graham (1997) *The Operational Auditing Handbook, Auditing Business Processes*, New York: John Wiley and Sons Inc., p. 16.
3. Ratliff Richard L, Wallace Wanda A, Sumners Glenn E, Mcfarland William G and Loebbecke James K (1996) *Internal Auditing, Principles and Techniques*, 2nd edition, Florida: The Institute of Internal Auditors, p. 17.
4. 'Profile – William Levant, doing it different'. *Internal Auditing and Business Risk*, pp. 24–27.
5. Krogstad Jack L., Ridgey Anthony J. and Rittenberg Larry E. 'Where we're going'. *Internal Auditing*, Jan. 2000, p. 24; 'Profile – William Levant, doing it different'. *Internal Auditing and Business Risk*, pp. 24–27.
6. Moeller Robert and Witt Herbert (1999) *Brink's Modern Internal Auditing*, 5th edition, Para. 1.7, New York: John Wiley and Sons Inc.
7. 'Ethics and the accountant in the public sector'. *ACCA*, March 1999, p. 51.
8. *The Guardian*, Thursday 3 Oct. 2002, p. 10, 'Fire unions call for member of pay review to quit', Maguire Kevin.
9. IS Auditing Guideline, Information Systems Audit and Control Association, Standard effective from 1 April 2002, Effect of Nonaudit Role on the IS Auditor Independence.
10. Mautz and Sharif (1961) *The Philosophy of Auditing*, American Accounting Association.
11. Courtemanche Gil (1986) *The New Internal Auditing*, New York: John Wiley and Sons Inc.
12. IIA.Inc. 'Audit independence and systems design' (1977).
13. Felten David, M. 'Objectivity – or else'. *Internal Auditor*, Feb. 1995, p. 30.
14. Rion Michael and Gebing Robert, K. 'Doing the right thing'. *Internal Auditor*, Dec. 1999, p. 33.
15. Eliason Michael 'Compliance plus integrity'. *Internal Auditor*, Dec. 1999, p. 30.
16. Marshall Alan 'So what do you do for a living?' *Internal Auditing*, May 1994, p. 17.
17. Flesher Dale (1996) *Internal Auditing: A One-Semester Course*, Florida: The Institute of Internal Auditors, p. 146.
18. *The Philosophy of Auditing* (1961) American Accounting Association.
19. CIPFA 'Perceptions of audit quality', April 1997, Executive Summary.
20. Churchill N. C. and Cooper W. W. (1965) 'A field study in internal auditing'. *The Accounting Review*, Vol. XL, No. 4.
21. Mints, F. E. (1972) 'Behavioural patterns in internal audit relationships', *IIA Research Paper 17*.
22. Hodge Neil 'View from the top'. *Internal Auditing and Business Risk*, Jan. 2001, pp. 14–18.
23. Filak Alicia J. 'Changing perceptions'. *Internal Auditor*, Oct. 2001, p. 80.
24. Sawyer Lawrence B. and Dittenhofer Mortimer A. assisted by Scheiner James H. (1996) *Sawyer's Internal Auditing*, 4th edition, Florida: The Institute of Internal Auditors, p. 1233.
25. Barrier Michale 'Retention keeping the best, the EBB and flow'. *Internal Auditor*, Oct. 2001, p. 33.
26. Leithhead Barry S. 'Putting CFIA in context'. *Internal Auditing*, April 2000, pp. 8–10.
27. *Internal Auditor*, Oct. 2001, p. 49.
28. IIA UK&IRELAND Professional guidance for internal auditors, Expressing an internal audit opinion, 2008.
29. OECD, Principles of Corporate Governance, revised May 2004, July 2006, p. 5 of 18, Evaluating whether companywide governance components work together as expected.
30. *Organizational Governance: Guidance for Internal Auditors*, July 2006, The Institute of Internal Auditors, Position Paper.
31. 'Towards a blueprint for the internal audit profession', Research by the Institute of Internal Auditors, p. 7 – UK and Ireland in association with Deloitte, Deloitte & Touche and the Institute of Internal Auditors – UK and Ireland 2008.
32. ICGN MEMBER RATIFICATION OF THE ICGN GLOBAL CORPORATE GOVERNANCE PRINCIPLES: REVISED (2009) 20 AUGUST 2009, ICGN GLOBAL CORPORATE GOVERNANCE PRINCIPLES: REVISED (2009), 6.6 Internal Audit.
33. *10 Risk Management Imperatives for Internal Auditing*, 2009, The Institute of Internal Auditors and its Audit Executive Center.
34. A New Agenda for Corporate Governance Reform, IIA UK&Ireland 2008, corporate governance reforms recommended by the Institute of Internal Auditors – UK and Ireland (IIA) in the wake of recent high-impact corporate financial scandals such as Enron, WorldCom and Xerox.
35. Wainwright Lisa 'Natwest audit'. *Internal Auditing*, Oct. 1998, p. 139.

Chapter 6

PROFESSIONALISM

Introduction

The internal auditor must be professional in the way work is planned and performed. This basic requirement involves a great deal of effort to ensure it is achieved and there are many sources of information that we can turn to for guidance in this respect. The ACCA argue that the term 'profession' suggests a grouping of people who have made a study of an area of knowledge or expertise and have achieved a level of competence in their chosen field.[1]

Internal audit is now a complete profession and features in most larger organizations in all sectors. This entails the use of competent staff, a respected role in the organization and robust QA arrangements that underpin the defined services that are provided. Note that all references to IIA defintions, code of ethics, IIA attribute and performance standards, practice advisories and practice guides relate to the IPPF prepared by the IIA in 2009. This chapter covers the following areas:

6.1 Audit Professionalism
6.2 Internal Auditing Standards
6.3 Due Professional Care
6.4 Professional Consulting Services
6.5 The Quality Concept
6.6 Defining the Client
6.7 Internal Review and External Review
6.8 Tools and Techniques
6.9 Marketing the Audit Role
6.10 Continuous Improvement
6.11 New Developments
Summary and Conclusions
Assignments and Multi-choice Questions

Various internal audit standards are listed to demonstrate the wide range of guidance that is available to the practising internal auditor. Note that the IIA International Standards for the Professional Practices of Internal Auditing is used extensively in the Handbook since the IIA is the only professional body that is dedicated to the specialist field of internal auditing.

6.1 Audit Professionalism

Internal auditing needs defined standards and this contributes to the development of professional audit services.

Can Standards Be Universal?

We have already established the fact that there are a variety of standards that cover internal auditing. Despite the real-life situation, it is nevertheless interesting to discuss the concepts of universality of standards and whether there are barriers to having one set of internal audit standards applicable throughout the world. The IIA has become a global organization and their standards have been adopted by all members in the various countries they are established in. Writers such as Gerald Vinten (taken from unpublished course notes from a Masters degree programme, City University Business School, 1991) have recognized the problems with international standards and some of the issues that relate to the question of universalism are now discussed:

1. Mandatory Should the standards be mandatory or just best practice, and if mandatory, should we accept that not all countries could comply? This also brings in the issue of how one might enforce mandatory standards across international boundaries. It may be better to set standards as targets that should be aimed at, as opposed to enforceable regulations. The problem arises where there is non-compliance and it is not clear whether any action should or can be taken. The world of external audit is fast moving towards the view that substandard work lowers the auditing profession's reputation and that firms must be policed as part of a review and certification process. This presumably will eventually be the case for the internal auditor in time to come to reinforce our claim that many sectors of society rely on our work. The contrasting view will argue that we cannot afford to be too rigid for audit units that are less able to meet professional standards.

2. Local factors How far do local factors affect the profession particularly where local legislation affects the role of internal auditing by setting out some of their compliance-based duties? Can one set of standards anticipate all such eventualities? It is clear that aspects of regulations in many countries envisage internal audit as having a major role in regularity audits as a safeguard against fraud. Where different countries have specific legislation that impacts on the audit role then it becomes even more difficult to set standards to any degree of detail. Furthermore, countries with large geographical areas and less developed communications systems may require their internal auditors to feedback basic information on these outstations. This information gathering function may be far removed from the professional risk-based systems approach that forms the basis of modern-day auditing.

3. Standardization To what extent should the standards require a standardized approach and how much flexibility should be built into discharging their requirements? Building on the above point, we would wish to create a balance between two competing positions in Figure 6.1.

There are ways that we can move closer towards this ideal:

- We must recognize the practicalities of real-life auditing and formulate standards that provide statements of intent rather than comprehensive procedures.
- Encourage each organization to translate the standards into suitable work practices and incorporate them into the audit manual.
- Make compliance with the spirit of the standards a major issue that is uppermost in the minds of all staff. To this end, any barriers to compliance should be addressed.

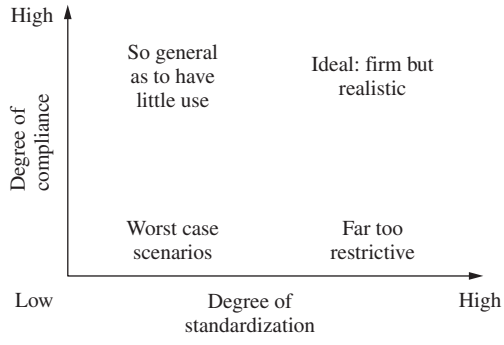


FIGURE 6.1 International internal auditing standards.

4. Translation The language problems and translation costs can be prohibitive. In fact it is sometimes difficult to find appropriate translations for certain words to convey the technical content and spirit of the matter being addressed. As a result, one dominant language (e.g. English) may reign supreme and so produce a slant towards the main language speakers.

5. Nationalism Nationalism and political manoeuvring can make life difficult. It may appear that a group of countries may possess most of the legislative powers with smaller, less developed countries more or less excluded from the main processes. Politics is almost unavoidable in any international forum and generally results in a disproportionate spread of power across member states. This may be the single most important factor in securing a level of agreement in terms of the universal application of auditing standards. It is clear that there are barriers to globalization although the IIA has made some ground in breaking them down. It is also questionable as to whether full standardization is a good thing, bearing in mind the different models of the internal audit role that exists throughout the world. What is more defensible is the view that there should be some agreement on the basic principles of internal audit, which form a fundamental base from which to promote the development of internal audit as a profession.

Notwithstanding the problem of securing a truly international dimension to internal auditing, the Global Institute of Internal Auditors seeks to represent a worldwide position. This exciting development may have a profound impact on the profession and is mentioned again in the final chapter of the Handbook.

Can Standards Apply to Smaller Organizations?

Internal audit standards set out ideals that should be striven for and in the main are based on healthy, growing audit departments with a CAE and a complement of full-time audit staff. Where the audit function consists of a person and a desk, the question arises as to whether standards can be applied in this situation:

1. Lower status Small audit departments may have a low status and therefore little of the necessary level of independence essential for the performance of good audit work. Most auditing

standards require that they are separate entities headed by a senior officer (e.g. a CAE). As such, small units located in an obscure part of the accountancy section may fall outside this requirement. It would be pointless to adopt standards that one knows cannot be achieved bearing in mind that any review of internal audit will comment on this non-compliance. Where internal audit is only recognized in terms of dual accountancy/audit posts, again problems with adopting IIA standards will ensue.

2. Type of work Smaller audit departments may be established essentially to provide extra resources for the external auditor and in this way be far removed from the models that the standards are based on. The audit work carried out may therefore be centred on testing routines and bear little resemblance to the modern audit role. Again independence may be compromised to the detriment of audit performance. Any move towards higher level risk-based auditing may be unattainable and standards that are based around this concept will be difficult to achieve. Where internal audit work programmes flow from external audit plans, standards that require the internal audit department to plan in its own name may be, in this scenario, unrealistic.

3. Level of expertise There may be a lack of certain expertise in areas necessary for a rounded collection of knowledge, skills and disciplines that may be essential to discharging a high-profile audit role. This may be true in areas such as computing, capital contracts, project management, management accountancy and so on. Audit training and development standards may be too far advanced for less developed auditing practices. Smaller audit departments may be at some disadvantage compared to larger ones. In fact, the audit function may be carried out by one sole person, far removed from the luxury of a structured, well-staffed internal audit department. Having said this, one may use internal auditing standards as professional targets that set the frame for the current audit function no matter how far this has developed to date. This holds so long as this is not used to criticize the efforts. In the final analysis the idea is that all audit departments are covered by the relevant standards and should attempt to comply as far as possible. It may well be the case that small but efficient/professional audit departments may become so successful that they eventually receive the support necessary for expansion.

The National Health Service (NHS) Experience

The role of internal auditing standards can be seen clearly in the way they were developed for the NHS in the UK. As a case study, it is interesting to consider how problems with an audit service were tackled through implementing suitable standards. A brief history may be set out as follows:

1. Although internal audit existed in parts of the NHS its role was not clearly defined.
2. A comptroller and auditor general reporting on the summarized accounts for 1979/80 noted various weaknesses in NHS internal audit including deficiencies in planning, reporting, computer coverage and low staffing numbers.
3. The Salmon Report of 1982 reviewed internal audit and made a number of major recommendations covering the role of audit and the approach to audit work. Besides staffing shortages, the low level of grades meant that professional standards were hard to attain.
4. As a result of these criticisms, an audit manual was issued in 1987 with a revised update version becoming mandatory from 1990.
5. 1994 – New *NHS Internal Audit Manual* and standards issued.
6. 1995 – An Accounting Officer's Memorandum is issued affirming the CEO's accountability. Guidance is issued on the organization and delivery of internal audit.

7. 1997–1998 – Health bodies are required to produce controls assurance statements in respect of internal financial controls to accompany the final accounts. Specific role of internal audit is to support and verify the process.
8. 1999 – Guidance is issued setting out risk management and organizational standards with the associated requirement to produce a controls assurance statement to accompany the annual report from 1999/2000. Internal audit is given specific responsibilities in this area in terms of verification and wider support.
9. 2000 – Treasury requirement for all departments to progress risk assessment processes relating to full statements of internal control.
10. 2002 – New set of internal auditing standards for the NHS.
11. The APB standards provided a framework but were not industry-specific, that is, tailored to the requirements of the NHS that were and still are going through major changes.
12. Besides setting qualitative standards, the manual also helped determine principles of coverage, raised expectations and raised the profile of specialist skills such as IS audit.

The preparation of NHS internal auditing standards is a direct response to external criticism of the need for a better direction and approach of the audit function. This point is made clear in the foreword to the standards. Although there has been some concern over the way staff have been developed to meet these new expectations, this is nonetheless a positive way of tackling the problem of poor performance. It is not enough simply to state that the IIA (or alternative) standards will be adopted. One must go on to formulate detailed guidance that relates to the specific circumstances of each individual business sector. The NHS standards are noted later on in this chapter.

Contribution of the Institute of Internal Auditors (IIA)

The main points relating to the contribution of the IIA are:

1. The IIA has developed a common body of knowledge that is examined before membership is acquired. In addition, it publishes a set of standards, a code of ethics and a statement of responsibilities. Each of these is dealt with in detail in separate parts of the Handbook.
2. The IIA has sanctions for dealing with breach of professional requirements and is now developing the mechanisms for enforcing them. Members have in the past been reprimanded for misconduct.
3. IIA members are not 'approved practitioners' as there is no requirement for CAEs to be qualified members. It would appear that anyone can be an internal auditor and sign off formal audit reports, although this will be subject to an individual organization's employment policies. In fact, there is a mistaken view that anyone can be an internal auditor without any training at all. This issue can be resolved at junior level but becomes more difficult where senior staff (with, say, contract or computing skills) are brought into internal audit with no intention of developing or understanding auditing skills. This reinforces the view that there is little or no use in employing unqualified people, or retaining those that are unable (or unwilling) to pass their auditing examinations or attend suitable training.
4. The professional practices framework contains a wealth of information and advice which is available to guide the composition and direction of internal auditing.
5. Internal auditors have not been sued for negligence and because of their position inside the organization, they are generally not exposed to this risk. This may alter as firms of accountants start to take on individual internal audit contracts where the internal audit function has been contracted out.

6. The IIA's research foundation provides a continuing source of material for developing the internal audit function of the future.

Standards play a crucial role in internal auditing and support the concept of auditing as a professionally based discipline. It is, however, clear that published statements are of little use unless they have been fully implemented and subject to continual review. The audit manual is the right mechanism for this process and it is through this that formal standards may be set and adopted. There are stringent tests that are applied to assessing whether a discipline has attained professional status and these revolve around the concept of providing a service to society in general. Internal audit may be referred to as a profession in its own right and the IIA and other versions of internal auditing standards are different in structure but are generally not inconsistent.

Hallmarks of Professionalism

Before studying the various standards attached to internal auditing, we consider the main features of a professional discipline:

1. Training programme A long specialized training programme that has to be undergone by the student before reaching practitioner status. This will typically last several years, covering topics that are dedicated to (or have a direct link with) the particular discipline. Architects, doctors, lawyers and accountants spend many years engaged in study and development before securing the full qualification.

2. Common body of knowledge A common body of knowledge (CBOK) attaches to the discipline and is to be mastered. This represents a minimum level of knowledge that is studied and understood. Some feel that the practitioner need not memorize an extensive range of facts as in practice one would have access to reference material. There is, though, a level of knowledge that should be at the instant recall of the practitioner. The extent to which various subjects are relevant to the discipline will have to be addressed when defining the content of the CBOK. The process of setting the CBOK will partly determine the boundaries of the profession and the areas considered important. The precise content may alter as the profession changes and adapts. For example, many professionals such as doctors and lawyers find it necessary to develop IT skills to use IS that promote greater efficiency in service delivery.

3. Code of ethics A code of ethics covering the required conduct expected from individual members of the profession. This is a fundamental requirement for all true professions in that it sets a moral framework within which individuals may practise. When one is acting as a professional, one in fact represents the entire profession. A suitable code of ethics will not only refer to the standards to which work will be performed, it will also set an overall code of conduct based around complete honesty and integrity as generalized concepts. This then sets the framework within which members are expected to conduct their affairs over and above mere compliance with the laws of the land. The invisible bond between the individual practitioner and the professional body allows a mutual trust that directs the respective activities of the two parties at all times.

4. Sanctions The sanction of the community applies to ensure that members perform to the required standards to form a formal bond between the profession and society in general. The hierarchical nature of professional standards might appear as Figure 6.2.

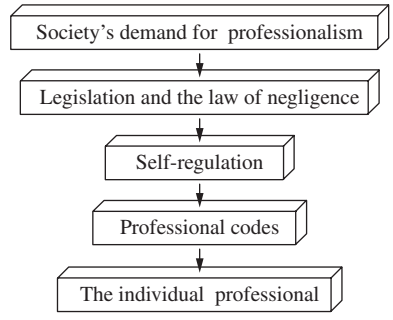


FIGURE 6.2 Business professionalism and society.

If the profession is unable to regulate itself, then society will resort to legislation to ensure that these demands are achieved. This is due to the importance of the services in question, in terms of their impact on society. Non-professionals will tend not to attract this degree of attention from society.

5. Control over services A professional person should be able to withdraw services where the situation is morally unacceptable. True professionals work to extremely high standards that cannot be compromised. If they were compromised, the individual should be in a position to withdraw from the situation.

6. Qualified practitioners The practice should be limited to qualified practitioners who have mastered the CBOK. Some form of licence would be issued. Licensed practitioners would be recognized by society as the only people allowed to carry out this type of work. This constitutes a formal barrier to the achievement of professional status as it is difficult to argue that a profession can be carried out by anyone without restriction. Many specialities will fail as a result of this principle. It is difficult to assess the extent to which formal qualifications are demanded as normal practice for a position in most organizations without carrying out research.

7. Morality The concept of morals over pure profits means that the discipline moves to a higher level above simple employment. Individuals should be practising through a desire to develop the profession and a wish to make a positive contribution, and would not be expected to hold a second job (as opposed to voluntary work) that is in any way related to the main role. The professional would be asked to work within the formal moral framework and not seek profit making as an overriding objective.

8. Technical difficulty The services provided should be technically difficult and this is linked to the concept of a CBOK. There should be some level of technical difficulty that has to be mastered through extensive training and several years' practical experience. If anyone can do the required work there is no justification for deeming the area as meeting the requirements of professionalism.

9. Examinations Formal examinations form part of the learning process in showing that the participant has acquired the various skills and techniques required. Although the extent to which examinations represent real-life situations that the practitioner will have to face is debatable, they remain an important component. The trend is towards course work and desktop training where

the link between studies and practice is more readily achieved. Formal exams are still a useful method of testing what has been learnt over a defined syllabus. They impose pressure which may emulate business pressures. The process of formulating the examinations' syllabus is useful for it forces one to define the scope of work and level of competence demanded.

10. Journals The publication of a journal and literature dedicated to the subject is another hallmark of professional status. One would expect to see a relevant monthly journal that contains technical updates and useful articles along with features on social meetings. Another main sign of professionalism is research studies that examine subjects of interest to members. These studies should result in changes to the direction and focus of the profession in specific areas. Textbooks play an important role, with major works representing academic standards in terms of providing a comprehensive coverage of relevant subject matter. It is difficult to visualize a profession unable to display a major range of textbooks.

11. Professional body A professional body represents the interests of its members and this is a prerequisite for many of the matters outlined above. We may wish to see

- a formal corporate status such as a company limited by guarantee;
- headquarters;
- a complement of full-time staff;
- a suitable logo;
- members' district societies;
- regular meetings and seminars/conferences;
- various committees to represent the interests of members;
- close contact with individual members;
- steps taken to commission research.

12. Compliance with rules The professional body would have to enforce various sanctions against members who failed to comply with any of the requirements of membership. One would wish to see a formal process (say with an ethics committee) to receive, consider and decide on cases referred to the professional body concerning the conduct of their members. There should be formal representation and an appeals process. The results of individual cases may be published in the journal, with or without names.

13. Service to society A major feature of a profession is the over-riding concept that its members are providing a service to society as opposed to individual clients. The ethos of the profession should be embodied in the view that it is there to fulfil an important role in society which is over and above the role it plays in servicing clients. Any conflict should be resolved by placing the duty of care to society first, which may serve to rule out many contenders who cannot show this.

Internal auditing is able to meet all of the above measures and is now firmly established as a professional discipline. This has been a huge achievement as ten to twenty years ago, it certainly was not the case. Having a firm professional base allows the internal audit community to plan for the future and track the way it needs to progress as its newly acquired high profile places it firmly on the boardroom agenda.

6.2 Internal Auditing Standards

The Institute of Internal Auditors (IIA)

The IIA has described its original objectives in 1941 when it was first established (www.theiiaorg.com):

> To cultivate, promote, and disseminate knowledge and information concerning internal auditing and subjects related thereto; to establish and maintain high standards of integrity, honor, and character among internal auditors; to furnish information regarding internal auditing and the practice and methods thereof to its members etc.

Since then the IIA has moved on to develop its PPF which contains the basic elements of the profession. It provides a consistent, organized method of looking at the fundamental principles and procedures that make internal auditing a unique, disciplined, and systematic activity. The purpose of the standards is to

1. delineate basic principles that represent the practice of internal auditing as it should be;
2. provide a framework for performing a broad range of value-added internal audit activities;
3. establish the basis for the measurement of internal audit performance;
4. foster improved organizational processes and operations.

The IPPF consists of:

International Standards for the Professional Practice of Internal Auditing which have to be followed by all practising (IIA) internal auditors.

Practice Advisories are pronouncements that are strongly recommended and endorsed by the IIA.

Note that the revisions of 2009 reduced the number of practice advisories down from 83 to 42. Position Papers deal with specific aspects of the governance and risk management agenda, while Practice Guides cover detailed guidance for carrying out internal audit activities.

The 2009 Standards now use the word "**must**" to mean an unconditional requirement and the word "**should**" where conformance is expected unless, when applying professional judgement, circumstances justify deviation.

The formal definition of internal audit is repeated for reference:

> Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

A main part of the IPPF is attribute and performance standards. Attribute standards describe the defining character of organizations and individuals performing internal audit services, while performance standards describe the nature of internal audit services and provide quality criteria against which to measure performance, and the individual implementation standards are used to augment the attribute and performance standards by helping employ them in particular types of

engagements. The 2009 International Standards for the Professional Practice of Internal Auditing cover both assurance services and client-based consulting and are set out below:

ATTRIBUTE STANDARDS

1000 – Purpose, Authority, and Responsibility

The purpose, authority, and responsibility of the internal audit activity must be formally defined in an internal audit charter, consistent with the Definition of Internal Auditing, the Code of Ethics, and the *Standards*. The chief audit executive must periodically review the internal audit charter and present it to senior management and the board for approval.

Interpretation:

The internal audit charter is a formal document that defines the internal audit activity's purpose, authority, and responsibility. The internal audit charter establishes the internal audit activity's position within the organization; authorizes access to records, personnel, and physical properties relevant to the performance of engagements; and defines the scope of internal audit activities. Final approval of the internal audit charter resides with the board.

1000.A1 – The nature of assurance services provided to the organization must be defined in the internal audit charter. If assurances are to be provided to parties outside the organization, the nature of these assurances must also be defined in the internal audit charter.

1000.C1 – The nature of consulting services must be defined in the internal audit charter.

1010 – Recognition of the Definition of Internal Auditing, the Code of Ethics, and the Standards in the Internal Audit Charter

The mandatory nature of the Definition of Internal Auditing, the Code of Ethics and the *Standards* must be recognized in the internal audit charter. The chief audit executive should discuss the Definition of Internal Auditing, the Code of Ethics, and the *Standards* with senior management and the board.

1100 – Independence and Objectivity

The internal audit activity must be independent, and internal auditors must be objective in performing their work.

Interpretation:

Independence is the freedom from conditions that threaten the ability of the internal audit activity or the chief audit executive to carry out internal audit responsibilities in an unbiased manner. To achieve the degree of independence necessary to effectively carry out the responsibilities of the internal audit activity, the chief audit executive has direct and unrestricted access to senior management and the board. This can be achieved through a dual-reporting relationship. Threats to independence must be managed at the individual auditor, engagement, functional, and organizational levels.

Objectivity is an unbiased mental attitude that allows internal auditors to perform engagements in such a manner that they believe in their work product and that no quality compromises are made. Objectivity requires that internal auditors do not subordinate their judgment on audit matters to others. Threats to objectivity must be managed at the individual auditor, engagement, functional, and organizational levels.

1110 – Organizational Independence

The chief audit executive must report to a level within the organization that allows the internal audit activity to fulfill its responsibilities. The chief audit executive must confirm to the board, at least annually, the organizational independence of the internal audit activity.

1110.A1 – The internal audit activity must be free from interference in determining the scope of internal auditing, performing work, and communicating results.

1111 – Direct Interaction with the Board

The chief audit executive must communicate and interact directly with the board.

1120 – Individual Objectivity

Internal auditors must have an impartial, unbiased attitude and avoid any conflict of interest.

Interpretation:

Conflict of interest is a situation in which an internal auditor, who is in a position of trust, has a competing professional or personal interest. Such competing interests can make it difficult to fulfill his or her duties impartially. A conflict of interest exists even if no unethical or improper act results. A conflict of interest can create an appearance of impropriety that can undermine confidence in the internal auditor, the internal audit activity, and the profession. A conflict of interest could impair an individual's ability to perform his or her duties and responsibilities objectively.

1130 – Impairment to Independence or Objectivity

If independence or objectivity is impaired in fact or appearance, the details of the impairment must be disclosed to appropriate parties. The nature of the disclosure will depend upon the impairment.

Interpretation:

Impairment to organizational independence and individual objectivity may include, but is not limited to, personal conflict of interest, scope limitations, restrictions on access to records, personnel, and properties, and resource limitations, such as funding.

The determination of appropriate parties to which the details of an impairment to independence or objectivity must be disclosed is dependent upon the expectations

of the internal audit activity's and the chief audit executive's responsibilities to senior management and the board as described in the internal audit charter, as well as the nature of the impairment.

1130.A1 – Internal auditors must refrain from assessing specific operations for which they were previously responsible. Objectivity is presumed to be impaired if an internal auditor provides assurance services for an activity for which the internal auditor had responsibility within the previous year.

1130.A2 – Assurance engagements for functions over which the chief audit executive has responsibility must be overseen by a party outside the internal audit activity.

1130.C1 – Internal auditors may provide consulting services relating to operations for which they had previous responsibilities.

1130.C2 – If internal auditors have potential impairments to independence or objectivity relating to proposed consulting services, disclosure must be made to the engagement client prior to accepting the engagement.

1200 – Proficiency and Due Professional Care

Engagements must be performed with proficiency and due professional care.

1210 – Proficiency

Internal auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively must possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities.

Interpretation:

Knowledge, skills, and other competencies is a collective term that refers to the professional proficiency required of internal auditors to effectively carry out their professional responsibilities. Internal auditors are encouraged to demonstrate their proficiency by obtaining appropriate professional certifications and qualifications, such as the Certified Internal Auditor designation and other designations offered by The Institute of Internal Auditors and other appropriate professional organizations.

1210.A1 – The chief audit executive must obtain competent advice and assistance if the internal auditors lack the knowledge, skills, or other competencies needed to perform all or part of the engagement.

1210.A2 – Internal auditors must have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization, but are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.

1210.A3 – Internal auditors must have sufficient knowledge of key information technology risks and controls and available technology-based audit techniques to perform their assigned work. However, not all internal auditors are expected to have the expertise of an internal auditor whose primary responsibility is information technology auditing.

1210.C1 – The chief audit executive must decline the consulting engagement or obtain competent advice and assistance if the internal auditors lack the knowledge, skills, or other competencies needed to perform all or part of the engagement.

1220 – Due Professional Care

Internal auditors must apply the care and skill expected of a reasonably prudent and competent internal auditor. Due professional care does not imply infallibility.

1220.A1 – Internal auditors must exercise due professional care by considering the:
- Extent of work needed to achieve the engagement's objectives;
- Relative complexity, materiality, or significance of matters to which assurance procedures are applied;
- Adequacy and effectiveness of governance, risk management, and control processes;
- Probability of significant errors, fraud, or noncompliance; and
- Cost of assurance in relation to potential benefits.

1220.A2 – In exercising due professional care internal auditors must consider the use of technology-based audit and other data analysis techniques.

1220.A3 – Internal auditors must be alert to the significant risks that might affect objectives, operations, or resources. However, assurance procedures alone, even when performed with due professional care, do not guarantee that all significant risks will be identified.

1220.C1 – Internal auditors must exercise due professional care during a consulting engagement by considering the:
- Needs and expectations of clients, including the nature, timing, and communication of engagement results;
- Relative complexity and extent of work needed to achieve the engagement's objectives; and
- Cost of the consulting engagement in relation to potential benefits.

1230 – Continuing Professional Development

Internal auditors must enhance their knowledge, skills, and other competencies through continuing professional development.

1300 – Quality Assurance and Improvement Program

The chief audit executive must develop and maintain a quality assurance and improvement program that covers all aspects of the internal audit activity.

Interpretation:

A quality assurance and improvement program is designed to enable an evaluation of the internal audit activity's conformance with the Definition of Internal Auditing and the Standards and an evaluation of whether internal auditors apply the Code of Ethics. The program also assesses the efficiency and effectiveness of the internal audit activity and identifies opportunities for improvement.

1310 – Requirements of the Quality Assurance and Improvement Program

The quality assurance and improvement program must include both internal and external assessments.

1311 – Internal Assessments

Internal assessments must include:

- Ongoing monitoring of the performance of the internal audit activity; and
- Periodic reviews performed through self-assessment or by other persons within the organization with sufficient knowledge of internal audit practices.

Interpretation:

Ongoing monitoring is an integral part of the day-to-day supervision, review, and measurement of the internal audit activity. Ongoing monitoring is incorporated into the routine policies and practices used to manage the internal audit activity and uses processes, tools, and information considered necessary to evaluate conformance with the Definition of Internal Auditing, the Code of Ethics, and the Standards.

Periodic reviews are assessments conducted to evaluate conformance with the Definition of Internal Auditing, the Code of Ethics, and the Standards.

Sufficient knowledge of internal audit practices requires at least an understanding of all elements of the International Professional Practices Framework.

1312 – External Assessments

External assessments must be conducted at least once every five years by a qualified, independent reviewer or review team from outside the organization. The chief audit executive must discuss with the board:

- The need for more frequent external assessments; and
- The qualifications and independence of the external reviewer or review team, including any potential conflict of interest.

Interpretation:

A qualified reviewer or review team consists of individuals who are competent in the professional practice of internal auditing and the external assessment process. The evaluation of the competency of the reviewer and review team is a judgment that considers the professional internal audit experience and professional credentials of the individuals selected to perform the review. The evaluation of qualifications also considers the size and complexity of the organizations that the reviewers have been associated with in relation to the organization for which the internal audit activity is being assessed, as well as the need for particular sector, industry, or technical knowledge.

An independent reviewer or review team means not having either a real or an apparent conflict of interest and not being a part of, or under the control of, the organization to which the internal audit activity belongs.

1320 – Reporting on the Quality Assurance and Improvement Program

The chief audit executive must communicate the results of the quality assurance and improvement program to senior management and the board.

Interpretation:

The form, content, and frequency of communicating the results of the quality assurance and improvement program is established through discussions with senior management and the board and considers the responsibilities of the internal audit activity and chief audit executive as contained in the internal audit charter. To demonstrate conformance with the Definition of Internal Auditing, the Code of Ethics, and the Standards, the results of external and periodic internal assessments are communicated upon completion of such assessments and the results of ongoing monitoring are communicated at least annually. The results include the reviewer's or review team's assessment with respect to the degree of conformance.

1321 – Use of "Conforms with the International Standards for the Professional Practice of Internal Auditing"

The chief audit executive may state that the internal audit activity conforms with the *International Standards for the Professional Practice of Internal Auditing* only if the results of the quality assurance and improvement program support this statement.

1322 – Disclosure of Nonconformance

When nonconformance with the Definition of Internal Auditing, the Code of Ethics, or the *Standards* impacts the overall scope or operation of the internal audit activity, the chief audit executive must disclose the nonconformance and the impact to senior management and the board.

PERFORMANCE STANDARDS

2000 – Managing the Internal Audit Activity

The chief audit executive must effectively manage the internal audit activity to ensure it adds value to the organization.

Interpretation:

The internal audit activity is effectively managed when:

- The results of the internal audit activity's work achieve the purpose and responsibility included in the internal audit charter;
- The internal audit activity conforms with the Definition of Internal Auditing and the Standards; and
- The individuals who are part of the internal audit activity demonstrate conformance with the Code of Ethics and the Standards.

2010 – Planning

The chief audit executive must establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organization's goals.

Interpretation:

The chief audit executive is responsible for developing a risk-based plan. The chief audit executive takes into account the organization's risk management framework, including using risk appetite levels set by management for the different activities or parts of the organization. If a framework does not exist, the chief audit executive uses his/her own judgment of risks after consultation with senior management and the board.

2010.A1 – The internal audit activity's plan of engagements must be based on a documented risk assessment, undertaken at least annually. The input of senior management and the board must be considered in this process.

2010.C1 – The chief audit executive should consider accepting proposed consulting engagements based on the engagement's potential to improve management of risks, add value, and improve the organization's operations. Accepted engagements must be included in the plan.

2020 – Communication and Approval

The chief audit executive must communicate the internal audit activity's plans and resource requirements, including significant interim changes, to senior management and the board for review and approval. The chief audit executive must also communicate the impact of resource limitations.

2030 – Resource Management

The chief audit executive must ensure that internal audit resources are appropriate, sufficient and effectively deployed to achieve the approved plan.

Interpretation:

Appropriate refers to the mix of knowledge, skills, and other competencies needed to perform the plan. Sufficient refers to the quantity of resources needed to accomplish the plan. Resources are effectively deployed when they are used in a way that optimizes the achievement of the approved plan.

2040 – Policies and Procedures

The chief audit executive must establish policies and procedures to guide the internal audit activity.

Interpretation:

The form and content of policies and procedures are dependent upon the size and structure of the internal audit activity and the complexity of its work.

2050 – Coordination

The chief audit executive should share information and coordinate activities with other internal and external providers of assurance and consulting services to ensure proper coverage and minimize duplication of efforts.

2060 – Reporting to Senior Management and the Board

The chief audit executive must report periodically to senior management and the board on the internal audit activity's purpose, authority, responsibility, and performance relative to its plan. Reporting must also include significant risk exposures and control issues, including fraud risks, governance issues, and other matters needed or requested by senior management and the board.

Interpretation:

The frequency and content of reporting are determined in discussion with senior management and the board and depend on the importance of the information to be communicated and the urgency of the related actions to be taken by senior management or the board.

2100 – Nature of Work

The internal audit activity must evaluate and contribute to the improvement of governance, risk management, and control processes using a systematic and disciplined approach.

2110 – Governance

The internal audit activity must assess and make appropriate recommendations for improving the governance process in its accomplishment of the following objectives:

- Promoting appropriate ethics and values within the organization;
- Ensuring effective organizational performance management and accountability;
- Communicating risk and control information to appropriate areas of the organization; and
- Coordinating the activities of and communicating information among the board, external and internal auditors, and management.

  2110.A1 – The internal audit activity must evaluate the design, implementation and effectiveness of the organization's ethics-related objectives, programs, and activities.

  2110.A2 – The internal audit activity must assess whether the information technology governance of the organization sustains and supports the organization's strategies and objectives.

  2110.C1 – Consulting engagement objectives must be consistent with the overall values and goals of the organization.

2120 – Risk Management

The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

Interpretation:

Determining whether risk management processes are effective is a judgment resulting from the internal auditor's assessment that:

- Organizational objectives support and align with the organization's mission;
- Significant risks are identified and assessed;
- Appropriate risk responses are selected that align risks with the organization's risk appetite; and
- Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.

Risk management processes are monitored through ongoing management activities, separate evaluations, or both.

2120.A1 – The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the:

- Reliability and integrity of financial and operational information.
- Effectiveness and efficiency of operations.
- Safeguarding of assets; and
- Compliance with laws, regulations, and contracts.

2120.A2 – The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.

2120.C1 – During consulting engagements, internal auditors must address risk consistent with the engagement's objectives and be alert to the existence of other significant risks.

2120.C2 – Internal auditors must incorporate knowledge of risks gained from consulting engagements into their evaluation of the organization's risk management processes.

2120.C3 – When assisting management in establishing or improving risk management processes, internal auditors must refrain from assuming any management responsibility by actually managing risks.

2130 – Control

The internal audit activity must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.

2130.A1 – The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organization's governance, operations, and information systems regarding the:

- Reliability and integrity of financial and operational information;
- Effectiveness and efficiency of operations;
- Safeguarding of assets; and
- Compliance with laws, regulations, and contracts.

2130.A2 – Internal auditors should ascertain the extent to which operating and program goals and objectives have been established and conform to those of the organization.

2130.A3 – Internal auditors should review operations and programs to ascertain the extent to which results are consistent with established goals and objectives to determine whether operations and programs are being implemented or performed as intended.

2130.C1 – During consulting engagements, internal auditors must address controls consistent with the engagement's objectives and be alert to significant control issues.

2130.C2 – Internal auditors must incorporate knowledge of controls gained from consulting engagements into evaluation of the organization's control processes.

2200 – Engagement Planning

Internal auditors must develop and document a plan for each engagement, including the engagement's objectives, scope, timing and resource allocations.

2201 – Planning Considerations

In planning the engagement, internal auditors must consider:

- The objectives of the activity being reviewed and the means by which the activity controls its performance;
- The significant risks to the activity, its objectives, resources, and operations and the means by which the potential impact of risk is kept to an acceptable level;
- The adequacy and effectiveness of the activity's risk management and control processes compared to a relevant control framework or model; and
- The opportunities for making significant improvements to the activity's risk management and control processes.

2201.A1 – When planning an engagement for parties outside the organization, internal auditors must establish a written understanding with them about objectives, scope, respective responsibilities, and other expectations, including restrictions on distribution of the results of the engagement and access to engagement records.

2201.C1 – Internal auditors must establish an understanding with consulting engagement clients about objectives, scope, respective responsibilities, and other client expectations. For significant engagements, this understanding must be documented.

2210 – Engagement Objectives

Objectives must be established for each engagement.

2210.A1 – Internal auditors must conduct a preliminary assessment of the risks relevant to the activity under review. Engagement objectives must reflect the results of this assessment.

2210.A2 – Internal auditors must consider the probability of significant errors, fraud, noncompliance and other exposures when developing the engagement objectives.

2210.A3 – Adequate criteria are needed to evaluate controls. Internal auditors must ascertain the extent to which management has established adequate criteria to determine whether

objectives and goals have been accomplished. If adequate, internal auditors must use such criteria in their evaluation. If inadequate, internal auditors must work with management to develop appropriate evaluation criteria.

2210.C1 – Consulting engagement objectives must address governance, risk management and control processes to the extent agreed upon with the client.

2220 – Engagement Scope

The established scope must be sufficient to satisfy the objectives of the engagement.

2220.A1 – The scope of the engagement must include consideration of relevant systems, records, personnel, and physical properties, including those under the control of third parties.

2220.A2 – If significant consulting opportunities arise during an assurance engagement, a specific written understanding as to the objectives, scope, respective responsibilities, and other expectations should be reached and the results of the consulting engagement communicated in accordance with consulting standards.

2220.C1 – In performing consulting engagements, internal auditors must ensure that the scope of the engagement is sufficient to address the agreed-upon objectives. If internal auditors develop reservations about the scope during the engagement, these reservations must be discussed with the client to determine whether to continue with the engagement.

2230 – Engagement Resource Allocation

Internal auditors must determine appropriate and sufficient resources to achieve engagement objectives based on an evaluation of the nature and complexity of each engagement, time constraints and available resources.

2240 – Engagement Work Program

Internal auditors must develop and document work programs that achieve the engagement objectives.

2240.A1 – Work programs must include the procedures for identifying, analyzing, evaluating and documenting information during the engagement. The work program must be approved prior to its implementation, and any adjustments approved promptly.

2240.C1 – Work programs for consulting engagements may vary in form and content depending upon the nature of the engagement.

2300 – Performing the Engagement

Internal auditors must identify, analyze, evaluate, and document sufficient information to achieve the engagement's objectives.

2310 – Identifying Information

Internal auditors must identify sufficient, reliable, relevant, and useful information to achieve the engagement's objectives.

Interpretation:

Sufficient information is factual, adequate, and convincing so that a prudent, informed person would reach the same conclusions as the auditor. Reliable information is the best attainable information through the use of appropriate engagement techniques. Relevant information supports engagement observations and recommendations and is consistent with the objectives for the engagement. Useful information helps the organization meet its goals.

2320 – Analysis and Evaluation

Internal auditors must base conclusions and engagement results on appropriate analyses and evaluations.

2330 – Documenting Information

Internal auditors must document relevant information to support the conclusions and engagement results.

2330.A1 – The chief audit executive must control access to engagement records. The chief audit executive must obtain the approval of senior management and/or legal counsel prior to releasing such records to external parties, as appropriate.

2330.A2 – The chief audit executive must develop retention requirements for engagement records, regardless of the medium in which each record is stored. These retention requirements must be consistent with the organization's guidelines and any pertinent regulatory or other requirements.

2330.C1 – The chief audit executive must develop policies governing the custody and retention of consulting engagement records, as well as their release to internal and external parties. These policies must be consistent with the organization's guidelines and any pertinent regulatory or other requirements.

2340 – Engagement Supervision

Engagements must be properly supervised to ensure objectives are achieved, quality is assured, and staff is developed.

Interpretation:

The extent of supervision required will depend on the proficiency and experience of internal auditors and the complexity of the engagement. The chief audit executive has

overall responsibility for supervising the engagement, whether performed by or for the internal audit activity, but may designate appropriately experienced members of the internal audit activity to perform the review. Appropriate evidence of supervision is documented and retained.

2400 – Communicating Results

Internal auditors must communicate the engagement results.

2410 – Criteria for Communicating

Communications must include the engagement's objectives and scope as well as applicable conclusions, recommendations, and action plans.

2410.A1 – Final communication of engagement results must, where appropriate, contain internal auditors' overall opinion and/or conclusions.

2410.A2 – Internal auditors are encouraged to acknowledge satisfactory performance in engagement communications.

2410.A3 – When releasing engagement results to parties outside the organization, the communication must include limitations on distribution and use of the results.

2410.C1 – Communication of the progress and results of consulting engagements will vary in form and content depending upon the nature of the engagement and the needs of the client.

2420 – Quality of Communications

Communications must be accurate, objective, clear, concise, constructive, complete and timely.

Interpretation:

Accurate communications are free from errors and distortions and are faithful to the underlying facts. Objective communications are fair, impartial, and unbiased and are the result of a fair-minded and balanced assessment of all relevant facts and circumstances. Clear communications are easily understood and logical, avoiding unnecessary technical language and providing all significant and relevant information. Concise communications are to the point and avoid unnecessary elaboration, superfluous detail, redundancy, and wordiness. Constructive communications are helpful to the engagement client and the organization and lead to improvements where needed. Complete communications lack nothing that is essential to the target audience and include all significant and relevant information and observations to support recommendations and conclusions. Timely communications are opportune and expedient, depending on the significance of the issue, allowing management to take appropriate corrective action.

2421 – Errors and Omissions

If a final communication contains a significant error or omission, the chief audit executive must communicate corrected information to all parties who received the original communication.

2430 – Use of "Conducted in Conformance with the International Standards for the Professional Practice of Internal Auditing"

Internal auditors may report that their engagements are "conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing*", only if the results of the quality assurance and improvement program support the statement.

2431 – Engagement Disclosure of Nonconformance

When nonconformance with the Definition of Internal Auditing, the Code of Ethics or the *Standards* impacts a specific engagement, communication of the results must disclose the:

- Principle or rule of conduct of the Code of Ethics or *Standard(s)* with which full conformance was not achieved;
- Reason(s) for nonconformance; and
- Impact of nonconformance on the engagement and the communicated engagement results.

2440 – Disseminating Results

The chief audit executive must communicate results to the appropriate parties.

Interpretation:

The chief audit executive or designee reviews and approves the final engagement communication before issuance and decides to whom and how it will be disseminated.

2440.A1 – The chief audit executive is responsible for communicating the final results to parties who can ensure that the results are given due consideration.

2440.A2 – If not otherwise mandated by legal, statutory, or regulatory requirements, prior to releasing results to parties outside the organization the chief audit executive must:

- Assess the potential risk to the organization;
- Consult with senior management and/or legal counsel as appropriate; and
- Control dissemination by restricting the use of the results.

2440.C1 – The chief audit executive is responsible for communicating the final results of consulting engagements to clients.

2440.C2 – During consulting engagements, governance, risk management, and control issues may be identified. Whenever these issues are significant to the organization, they must be communicated to senior management and the board.

2500 – Monitoring Progress

The chief audit executive must establish and maintain a system to monitor the disposition of results communicated to management.

2500.A1 – The chief audit executive must establish a follow-up process to monitor and ensure that management actions have been effectively implemented or that senior management has accepted the risk of not taking action.

2500.C1 – The internal audit activity must monitor the disposition of results of consulting engagements to the extent agreed upon with the client.

2600 – Resolution of Senior Management's Acceptance of Risks

When the chief audit executive believes that senior management has accepted a level of residual risk that may be unacceptable to the organization, the chief audit executive must discuss the matter with senior management. If the decision regarding residual risk is not resolved, the chief audit executive must report the matter to the board for resolution.

THE IIA CODE OF ETHICS

The purpose of the Institute's Code of Ethics is to promote an ethical culture in the profession of internal auditing. A code of ethics is necessary and appropriate for the profession of internal auditing, founded as it is on the trust placed in its objective assurance about risk management, control and governance. The Institute's Code of Ethics extends beyond the definition of internal auditing to include two essential components:

1. Principles that are relevant to the profession and practice of internal auditing.
2. Rules of conduct that describe behaviour norms expected of internal auditors.

Principles

Internal auditors are expected to apply and uphold the following principles:

1. Integrity
The integrity of internal auditors establishes trust and thus provides the basis for reliance on their judgment.

2. Objectivity
Internal auditors exhibit the highest level of professional objectivity in gathering, evaluating and communicating information about the activity or process being examined. Internal auditors make a balanced assessment of all the relevant circumstances and are not unduly influenced by their own interests or by others in forming judgments.

3. Confidentiality

Internal auditors respect the value and ownership of information they receive and do not disclose information without appropriate authority unless there is a legal or professional obligation to do so.

4. Competency

Internal auditors apply the knowledge, skills and experience needed in the performance of internal audit services.

Rules of Conduct:

1. Integrity

Internal auditors:

1.1. Shall perform their work with honesty, diligence, and responsibility.

1.2. Shall observe the law and make disclosures expected by the law and the profession.

1.3. Shall not knowingly be a party to any illegal activity, or engage in acts that are discreditable to the profession of internal auditing or to the organization.

1.4. Shall respect and contribute to the legitimate and ethical objectives of the organization.

2. Objectivity

Internal auditors:

2.1. Shall not participate in any activity or relationship that may impair or be presumed to impair their unbiased assessment. This participation includes those activities or relationships that may be in conflict with the interests of the organization.

2.2. Shall not accept anything that may impair or be presumed to impair their professional judgment.

2.3. Shall disclose all material facts known to them that, if not disclosed, may distort the reporting of activities under review.

3. Confidentiality

Internal auditors:

3.1. Shall be prudent in the use and protection of information acquired in the course of their duties.

3.2. Shall not use information for any personal gain or in any manner that would be contrary to the law or detrimental to the legitimate and ethical objectives of the organization.

4. Competency

Internal auditors:

4.1. Shall engage only in those services for which they have the necessary knowledge, skills, and experience.

4.2. Shall perform internal audit services in accordance with the *International Standards for the Professional Practice of Internal Auditing*.

4.3. Shall continually improve their proficiency and the effectiveness and quality of their services.

Chartered Institute of Public Finance and Accountancy (CIPFA) Standards

Building on the 1990 APB internal audit code, and their 78 paragraph code from 2002, CIPFA has prepared a code of practice for internal audit that forms a good framework for the local

government sector. Andy Wynne has provided an insight into the background to local government internal auditing:

> But the real argument is whether internal audit is part of the internal control system or is responsible for reviewing that system. Certainly, the role of internal audit has changed over time. When first introduced into local government, it was definitely part of the internal control system; its remit was to undertake regular checks on large samples of financial transactions. So, in 1936, it was defined in Audits of Local Authorities, as 'an organised arrangement for securing a continuous and thorough check upon the financial transactions of local authority'. Echoes of this role are still to be seen in some local authorities where the final accounts of capital contracts are not paid until they had been checked and cleared by internal audit. The first major development was the systems approach.[2]

Extracts from the 2003 CIPFA code on Internal Audit Standards for Local Government in the UK follow:

Definition of Internal Audit

Internal audit is an independent and objective appraisal service within an organisation:

Internal audit is an assurance function that primarily provides an independent and objective opinion to the organisation on the degree to which the internal control environment supports the achievement of the organisation's objectives. The internal control environment comprises the policies, procedures and operations established to ensure the achievement of objectives, the appropriate assessment of risk, the reliability of internal and external reporting and accountability processes, compliance with applicable laws and regulations, and compliance with the behavioural and ethical standards set for the organisation. In addition, internal audit's findings and recommendations are beneficial to line management in the audited areas. Internal audit can also provide an independent and objective consultancy service specifically to help line management improve the organisation's internal control environment. The service applies the professional skills of internal audit through a systematic and disciplined evaluation of the policies, procedures and operations that management put in place to ensure the achievement of the organisation's objectives, and through recommendations for improvement. Such consultancy work can contribute to the opinion which internal audit provides on the internal control environment.

Code of Ethics for Internal Auditors

The purpose of this code of ethics is to set the minimum standards for the performance and conduct of all internal auditors. This code is intended to clarify the standard of conduct expected from all members of internal audit when carrying out their duties. The code applies to all staff responsible for delivering internal audit within local government, but does not supersede or replace the requirement on individuals to comply with ethical codes issued by professional institutes of which they are members or student members and any organisational codes of ethics/conduct. There are four main principles that should be observed.

1. Integrity
2. Objectivity

3. Competency
4. Confidentiality

Organisational Standards

1. Scope of Internal Audit The purpose, authority and responsibility of internal audit should be formally defined by the organisation in Terms of Reference. Internal Audit should fulfil its terms of reference by systematic review and evaluation of the internal control environment which comprises the policies, procedures and operations in place to:

- establish, and monitor the achievement of, the organisation's objectives;
- identify, assess and manage the risks to achieving the organisation's objectives;
- advise on, formulate and evaluate policy;
- ensure the economical, effective and efficient use of resources;
- ensure compliance with established policies (including behavioural and ethical expectations), procedures, laws and regulations;
- safeguard the organisation's assets and interests from losses of all kinds, including those arising from fraud, irregularity or corruption;
- ensure the integrity and reliability of information, accounts and data, including internal and external reporting and accountability processes.

2. Independence Internal audit should be sufficiently independent of the activities, which it audits to enable auditors to perform their duties in a manner, which facilitates impartial and effective professional judgements and recommendations. Internal auditors should have no executive responsibilities.

Subject to any over-riding statutory responsibilities of the Responsible Financial Officer or any over-riding instructions by the organisation, accountability for the response to the advice and recommendations of internal audit lies with the line managers who either accept and implement the advice or formally reject it. Audit advice and recommendations are without prejudice to the right of internal audit to review the relevant policies, procedures and operations at a later date.

3. Audit Committees Internal Audit in Local Government must report to elected members. How this is achieved is for the organisation to decide. Where the Code refers to Audit Committees this should be read in the context of the specific mechanism for reporting to members that exists in the organisation. This Standard only encompasses internal audit issues and does not define the full role or constitution of an Audit Committee.

4. Relationships with Management, Other Auditors and Other Review Bodies The Head of Internal Audit should co-ordinate internal audit plans and activities with line managers, other internal auditors, external audit, inspection bodies and other review agencies to ensure the most effective audit coverage is achieved and duplication of effort is minimised.

5. Staffing, Training and Development Internal Audit should be appropriately staffed in terms of numbers, grades, qualification levels and experience, having regard to its objectives and to these standards. Internal auditors should be properly trained to fulfil their responsibilities and should maintain their professional competence through an appropriate ongoing development programme.

Operational Standards

6. Audit Strategy The audit strategy is the high level concept of how the internal audit service will be delivered and developed. It can be presented as a document in its own right or integrated into an existing document, such as the business/service plan.

7. Management of Audit Assignments For each audit assignment a detailed brief should be prepared and discussed with relevant line managers. These briefs should establish detailed objectives for the assignment, resource requirements, audit outputs and target dates. They should set out:

- the scope and objectives of the work to be done
- any issues which line management would like addressed during the audit
- reporting arrangements
- the timing of the assignment and the budget
- staff allocation and supervision arrangements

8. Due Professional Care Due professional care is the care and skill that a reasonably prudent and competent internal auditor will apply in performing their duties.

- Due care is working with competence and diligence. It does not imply infallibility.
- Due professional care is the use of audit skills and judgement based on appropriate experience, training (including continuing professional development), ability, integrity and objectivity.
- Due professional care should be appropriate to the objectives, complexity, nature and materiality of the audit being performed.
- Due professional care is achieved by adherence to these standards.

9. Reporting The Head of Internal Audit should determine the way in which assurance and consultancy findings will be reported, subject to the provisions of these standards and the requirements of the Responsible Financial Officer, the Audit Committee and any third parties.

- The Head of Internal Audit should set local standards for all reports.
- Internal Audit should agree with report recipients the form and medium of those reports.
- All audit findings should be promptly reported.
- The Head of Internal Audit should provide a written report to the Responsible Financial Officer timed to support the Statement on Internal Control.
- The Head of Internal Audit should be entitled to report any control, governance or risk management issue directly to the Responsible Financial Officer.

10. Quality Assurance The work of internal audit should be controlled at each level of operation to ensure that a continuously effective level of performance, compliant with these standards, is being maintained. The Head of Internal Audit should develop a quality assurance programme designed to gain assurance by both internal and external review that the work of internal audit is compliant with these standards and achieves its objectives, and to sustain a commentary on compliance with these standards in the annual audit report.

CIPFA update their code of practice in a regular basis and their 2006 definition of internal auditing reads as follows:

> "an assurance function that provides an independent and objective opinion to the organisation on the control environment (the systems of governance, risk management and internal control), by evaluating its effectiveness in achieving the organisation's objectives. It objectively examines, evaluates and reports on the adequacy of the control environment as a contribution to the proper, economic, efficient and effective use of resources."

Government Internal Auditing Standards

The Treasury has a section dedicated to central government internal auditing called Assurance, Control and Risk (ACR) and their objectives for 2002–2003 were as follows:

1. Promote greater accountability through the implementation of corporate governance and a resource based financial management system.
2. Promote high standards of regularity, propriety and accountability through an appropriately skilled and resourced internal audit service. ACR seeks to improve the quality of internal audit across government and supports internal audit in the delivery of their risk management, control and governance service.
3. Promoting high standards of regularity and propriety through maintaining an awareness of fraud and the development of an anti-fraud culture across government.
4. Promoting an awareness internationally and within Europe of UK financial management and audit.

Government Accounting requires Accounting Officers, in accordance with their terms of appointment, to make provision for internal audit in accordance with the standards set out in the *Government Internal Audit Manual*. The Government Internal Audit Standards were revised in July 2001 and cover the following areas:

Definition of Internal Audit Internal audit is an independent and objective appraisal service within an organisation:

- Internal audit primarily provides an independent and objective opinion to the Accounting Officer on risk management, control and governance, by measuring and evaluating their effectiveness in achieving the organisation's agreed objectives. In addition, internal audit's findings and recommendations are beneficial to line management in the audited areas. Risk management, control and governance comprise the policies, procedures and operations established to ensure the achievement of objectives, the appropriate assessment of risk, the reliability of internal and external reporting and accountability processes, compliance with applicable laws and regulations, and compliance with the behavioural and ethical standards set for the organisation.
- Internal audit also provides an independent and objective consultancy service specifically to help line management improve the organisation's risk management, control and governance. The service applies the professional skills of internal audit through a systematic and disciplined evaluation of the policies, procedures and operations that management put in place to ensure the achievement of the organisation's objectives, and through recommendations for

improvement. Such consultancy work contributes to the opinion which internal audit provides on risk management, control and governance.

The Code of Ethics for Internal Auditors in Central Government requires the observance of four main principles:

1. Integrity
2. Objectivity
3. Competency
4. Confidentiality

A list of the areas covered in the organisational and operational standards follows:

Organisational standards:

1. Scope of Internal Audit
- 1.1 Provision of Terms of Reference
- 1.2 Scope of work
- 1.3 Responsibilities in respect of other bodies
- 1.4 Fraud

2. Independence
- 2.1 The principles of independence
- 2.2 Organisational independence
- 2.3 Status of the Head of Internal Audit
- 2.4 Independence of individual auditors
- 2.5 Independence of audit contractors
- 2.6 Declaration of conflict of interest

3. Audit Committees
- 3.1 Principles of the Audit Committee
- 3.2 Internal Audit issues on which the Accounting Officer should seek the Audit Committee's advice
- 3.3 The Head of Internal Audit's relationship with the Audit Committee

4. Relationships with Management, Other Auditors and Other Review Bodies
- 4.1 Principles of good relationships
- 4.2 Relationships with management
- 4.3 Relationships with other internal auditors
- 4.4 Relationships with external auditors
- 4.5 Relationships with other review bodies

5. Staffing, Training and Development
- 5.1 Principles of staffing, training and development
- 5.2 The Government Internal Audit Certificate
- 5.3 Staffing the Internal Audit Unit
- 5.4 Continuing Professional Development

Operational standards:

6. Audit Strategy
- 6.1 Developing the internal audit strategy
- 6.2 Developing the periodic audit plans

7. Management of Audit Assignments
- 7.1 Planning

7.2 Approach
7.3 Follow-up

8. Due Professional Care
8.1 Principles of due professional care
8.2 Conduct of the individual auditor
8.3 Organisational arrangements for due professional care

9. Reporting
9.1 Principles of reporting
9.2 Assignment recording and reporting
9.3 Annual reporting and presentation of audit opinion

10. Quality Assurance
10.1 Principles of Quality Assurance
10.2 Management of internal audit
10.3 Internal quality review
10.4 External quality review

National Health Service (NHS) Standards

All NHS organizations are required to make provision for internal audit in accordance with these standards. The definition of internal audit and accompanying standards for the professional practice of internal audit in NHS organizations are addressed to accountable officers, boards, directors of finance, audit committees and to heads of internal audit. The definition and standards have been updated to ensure alignment with the Government Internal Audit Standards. The 2002 version replaces the standards issued by the NHS Executive in 1995. The NHS definition of internal audit follows:

> Internal audit is an independent and objective appraisal service within an organisation. Internal audit primarily provides an independent and objective opinion to the Accountable Officer, the Board and the Audit Committee on the degree to which risk management, control and governance support the achievement of the organisation's agreed objectives. In addition, internal audit's findings and recommendations are beneficial to line management in the audited areas. Risk management, control and governance comprise the policies, procedures and operations established to ensure the achievement of objectives, the appropriate assessment of risk, the reliability of internal and external reporting and accountability processes, compliance with applicable laws and regulations, and compliance with the behavioural and ethical standards set for the organisation. Internal audit also provides an independent and objective consultancy service specifically to help line management improve the organisation's risk management, control and governance. The service applies the professional skills of internal audit through a systematic and disciplined evaluation of the policies, procedures and operations that management put in place to ensure the achievement of the organisation's objectives, and through recommendations for improvement. Such consultancy work contributes to the opinion which internal audit provides on risk management, control and governance. Audit work designed to deliver opinion on the risk management, control and governance of the organisation is referred to in these standards as 'assurance work' because management use the audit opinion to derive assurance about the effectiveness of their controls.

Code of ethics for internal auditors:

1. Integrity
2. Objectivity

3. Competency
4. Confidentiality

Organisational standards

Scope of Internal Audit The purpose, authority and responsibility of internal audit should be formally defined by the organisation in Terms of Reference.

Independence Internal audit should be sufficiently Independent of the activities, which it audits to enable auditors to perform their duties in a manner, which facilitates impartial and effective professional judgements and recommendations. Internal auditors should have no executive responsibilities.

Audit Committees Every NHS Trust is required to establish a non-executive committee of the Board to be known as the Audit Committee. The main objective of that Committee is to Independently contribute to the Board's overall process for ensuring that an effective internal control system is maintained. The primary focus of this work has historically related to Internal financial control matters such as the safeguarding of assets, the maintenance of proper accounting records and the reliability of financial Information. With the requirement to make wider Statements on Internal Control Boards are increasingly looking to Audit Committees to provide assurance on the arrangements relating to all internal control activities.

Relationships with Management, Other Auditors and Other Review Bodies Heads of Internal Audit should co-ordinate internal audit plans and activities with line managers, other internal auditors, external audit and other review agencies to ensure the most effective audit coverage is achieved and duplication of effort is minimized.

Staffing, Training and Development Internal Audit should be appropriately staffed in terms of numbers, grades, qualification levels and experience, having regard to its objectives and to these standards. Internal auditors should be property trained to fulfil their responsibilities and should maintain their professional competence through an appropriate ongoing development programme.

Operational standards

Audit Strategy The Head of Internal Audit should develop and maintain a strategy for providing the Accountable Officer, economically and efficiently, with objective evaluation of, and opinions on, the effectiveness of the organisation's risk management, control and governance arrangements. The Head of Internal Audit's opinions are a key element of the framework of assurance, and the Accountable Officer needs to inform the completion of the annual SIC.

Management of Audit Assignments For each audit assignment a detailed plan should be prepared and discussed with relevant line managers. Any material objection to the assignment plans, which cannot be resolved by negotiation, should be referred to the Audit Committee. These plans should establish detailed objectives for the assignment, the level of assurance that

management wishes to derive from the opinion to be delivered, resource requirements, audit outputs and target dates.

Due Professional Care Due professional care is the care and skill that a reasonably prudent and competent internal auditor will apply in performing their duties.

Reporting The Head of Internal Audit should determine the way in which audit findings will be reported, subject to the provisions of these standards and the requirements of the Accountable Officer, the Audit Committee and any third parties.

Quality Assurance The work of internal audit should be controlled at each level of operation to ensure that a continuously effective level of performance compliant with these standards is being maintained. The Head of Internal Audit should develop a quality assurance programme designed to gain assurance by both internal and external review that the work of internal audit is compliant with these standards and achieves its objectives, and to sustain a commentary on compliance with these standards in the annual audit report.

6.3 Due Professional Care

Taking care during the audit process is becoming an increasingly onerous requirement for the internal auditor. The dismissal of two internal auditors by Allied Irish Bank's US subsidiary (Allfirst) in the wake of the activities of rogue trader John Rusnak provides a powerful illustration of the concept of due professional care. The need to take care is reinforced by Attribute Standard 1220 (Due Professional Care) which states that internal auditors must apply the care and skill expected of a reasonably prudent and competent internal auditor. Due professional care does not imply infallibility. Standard 1220.A1 goes on to say that the internal auditor should consider the:

- Extent of work needed to achieve the engagement's objectives.
- Relative complexity, materiality, or significance of matters to which assurance procedures are applied.
- Adequacy and effectiveness of risk management, control, and governance processes.
- Probability of significant errors, irregularities, or noncompliance.
- Cost of assurance in relation to potential benefits.

In determining whether standards have been met there is help at hand. IIA standard 1200 covers proficiency and due professional care by stating that:

> Engagements must be performed with proficiency and due professional care.

The IIA Practice Advisory 1220-1 (Proficiency and Due Professional Care) suggests that:

- Proficiency and due professional care are the responsibility of the chief audit executive (CAE) and each internal auditor. As such, the CAE ensures that persons assigned to each engagement collectively possess the necessary knowledge, skills, and other competencies to conduct the engagement appropriately.
- Due professional care includes conforming with the Code of Ethics and, as appropriate, the organization's code of conduct as well as the codes of conduct for other professional

designations the internal auditors may hold. The Code of Ethics extends beyond the Definition of Internal Auditing to include two essential components:

- Principles that are relevant to the profession and practice of internal auditing: integrity, objectivity, confidentiality, and competency.
- Rules of conduct that describe behavioral norms expected of internal auditors. These rules are an aid to interpreting the principles into practical applications and are intended to guide the ethical conduct of internal auditors.

Consulting work is also covered by the need for care and Attribute Standard 1220.C1 argues that care in consulting work is exercised:

> The chief audit executive must decline the consulting engagement or obtain competent advice and assistance if the internal auditors lack the knowledge, skills, or other competencies needed to perform all or part of the engagement.

Due care is a duty that runs throughout the internal audit shop and also for work commissioned by the internal auditor. Where outsiders are used to support the internal audit work, the need to exercise care in managing the arrangement is reflected in IIA Practice Advisory 1210.A1-1 (Obtaining External Services to Support or Complement the Internal Audit Activity). Primary standard 1210.A1 states that:

> The chief audit executive must obtain competent advice and assistance if the internal auditors lack the knowledge, skills, or other competencies needed to perform all or part of the engagement.

Practice Advisory 1210.A1-1 makes the following suggestions:

1. Each member of the internal audit activity need not be qualified in all disciplines. The internal audit activity may use external service providers or internal resources that are qualified in disciplines such as accounting, auditing, economics, finance, statistics, information technology, engineering, taxation, law, environmental affairs, and other areas as needed to meet the internal audit activity's responsibilities.
2. An external service provider is a person or firm, independent of the organization, who has special knowledge, skill, and experience in a particular discipline. External service providers include actuaries, accountants, appraisers, culture or language experts, environmental specialists, fraud investigators, lawyers, engineers, geologists, security specialists, statisticians, information technology specialists, the organization's external auditors, and other audit organizations. An external service provider may be engaged by the board, senior management, or the chief audit executive (CAE).
3. External service providers may be used by the internal audit activity in connection with, among other things:
   - Achievement of the objectives in the engagement work schedule.
   - Audit activities where a specialized skill and knowledge are needed such as information technology, statistics, taxes, or language translations.
   - Valuations of assets such as land and buildings, works of art, precious gems, investments, and complex financial instruments.
   - Determination of quantities or physical condition of certain assets such as mineral and petroleum reserves.
   - Measuring the work completed and to be completed on contracts in progress.
   - Fraud and security investigations.

- Determination of amounts, by using specialized methods such as actuarial determinations of employee benefit obligations.
- Interpretation of legal, technical, and regulatory requirements.
- Evaluation of the internal audit activity's quality assurance and improvement program in conformance with the Standards.
- Mergers and acquisitions.
- Consulting on risk management and other matters.

As a shortcut to isolating the principles upon which the elements of an audit are based, we may seek to devise a model in Figure 6.3.

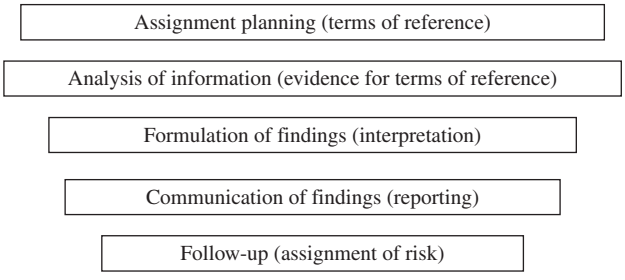


FIGURE 6.3 Model of baseline standards.

Each individual audit has to meet a set of baseline standards if it is to be of acceptable quality, and as such, the components outlined above will have to be firmly in place. If this is not the case then there is a strong argument to conclude that the audit has not been performed properly. We can go on to state that where this is the norm for most audits then the audit function itself can in no way be proficient. In this instance, the CAE, if a member of a professional auditing body, should be disciplined by the professional body. This simple formula should be firmly in place or there is little hope for developing the practice of internal auditing. In this sense it may be the case that all chief auditors need to be members of an appropriate professional auditing body. We have shown that there are mechanisms that must be in place to satisfy the auditing standards that cover the performance of audit work. One acid test is to ask whether the procedures covering this issue would stand up in a court of law that wished to consider whether an audit had been performed to acceptable standards. Although this point is more relevant to firms of external auditors, it should nonetheless be noted by internal auditors as more public sector internal audit functions are being contracted out. Professional standards emphasize a disciplined approach to the auditor's duties and work that is derived from best practice. In addition, the various requirements call for a professional approach to auditing where the work is planned, based on good evidence, reported and followed up. The move towards risk-based auditing has gained ground and it may be suggested that professional audit work should reflect this fact. Some writers argue that the future of internal auditing is based on understanding risk management:

> All too often internal auditors . . . are fighting against the full and proper implementation of risk management into their organisations . . . :
>
> - internal auditors have a tendency to recommend highly risk averse processes and procedures through their own risk taking preferences and demanding that areas of their business build upon layer upon layer of internal control over relatively risk free areas of the business.

- internal auditors are frequently not aware of the organisational preferences for risk taking . . .
- internal auditors regularly fail to get sufficiently close to the strategic opportunities and challenges that their organisations are working on and working towards.
- even when they are being more forward looking they still fail to allow line management and their staff to take ownership for risk and risk management – which is the only effective way that it will work.[3]

An audit department that does not establish suitable procedures to take on board all these matters cannot discharge the requirements of professional standards. In addition, the audit department must be staffed with personnel who between them have all the skills required to discharge the audit role. These skills are varied and cover a range of disciplines based on the whole body of audit knowledge, which is studied during professional auditing examinations. If the CAE does not ensure that these skills are employed or readily available then professional auditing standards cannot be met. There may be a case for having internal audit functions that are able to meet performance standards, formally designated as 'certificated internal auditors'. This is in contrast to other audit functions that have no such allegiance or are unable to meet the required standards. Nothing short of this will raise auditing standards to a level where they have any real purpose. We can also take the view that the current search for QA 'Kitemarks' may become a thing of the past. The audit function will simply rely on statements to the effect that they are in compliance with professional standards as the chief marketing tool. Again taking a futuristic view of this position, we may move towards the quality control mechanism applied to professional internal audit units as a means of accrediting the audit service as shown in Figure 6.4.

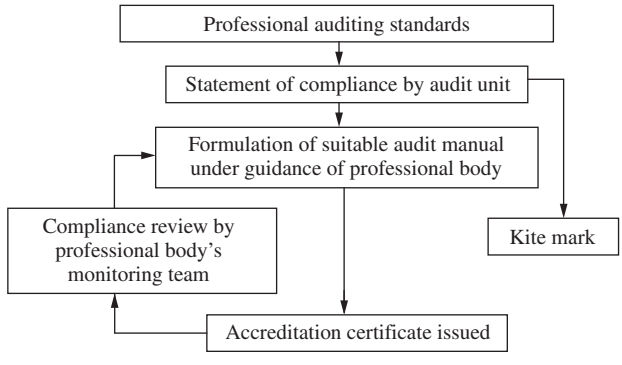


FIGURE 6.4 Monitoring performance standards.

This is a simple concept which in reality requires some rethinking by the internal auditor in terms of seeking a full professional affiliation, along with a degree of additional resources where professional bodies seek to perform this new role. Professionalism is based on the continual search for new knowledge. To this end, the IIA Research Foundation was founded in 1976 and has embarked on a continuous drive for probing the future of internal auditing. The Foundation's main objectives include:

> To support research and education in internal auditing and generally to promote the internal auditing profession. It accomplishes this in the following way:
>
> - Provide grants to individuals or organizations to undertake worthwhile projects in research or educational areas that will further the profession.

- Conducting forums, educating practitioners, scholars, and the general public in specific internal auditing areas.
- Awarding grants and certificates to increase the knowledge of internal auditing practitioners, scholars, and the general public at large.
- Administering pamphlets, books, monographs, and other educational materials for use by individuals, schools, libraries, organizations and the general public.[4]

6.4 Professional Consulting Services

The definition of internal auditing makes it clear that it is an assurance and consulting activity. The IIA has defined an assurance service as:

> An objective examination of evidence for the purpose of providing an independent assessment of risk management, control, or governance processes for the organisation. Examples may include financial, compliance, systems security, and due diligence engagements.

Consulting services are defined by the IIA as:

> Advisory and related client service activities, the nature and scope of which are agreed with the client, are intended to add value and improve an organization's governance, risk management, and control processes without the internal auditor assuming management responsibility. Examples include counsel, advice, facilitation, and training.

The primary players in assurance work are the auditor, the client and the third party to whom assurance is being provided, while for consulting work it is simply the auditor and the client. Assurance work is well understood by the internal audit community and over the years there has been 'creeping consulting' normally in the form of advice and information on request from the line managers. What has not happened before is the offer of a formal consulting service based around the corporate governance, risk management and control dimensions. Many auditors simply suggest that they will do more consulting work, but may not appreciate that this is an entire industry, with set standards and methods, many of which are similar to internal audit techniques. The IIA has helped with guidance on consulting to help set the scene. Consulting standard **1130.C1** states:

> Internal auditors may provide consulting services relating to operations for which they had previous responsibilities.

Standard 1130.C2 goes on to say:

> If internal auditors have potential impairments to independence or objectivity relating to proposed consulting services, disclosure must be made to the engagement client prior to accepting the engagement.

Practice Advisory 1120-1 covers individual objectivity and there is advice on what does and what does not impair objectivity:

> The internal auditor's objectivity is not adversely affected when the auditor recommends standards of control for systems or reviews procedures before they are implemented. The auditor's objectivity is considered to be impaired if the auditor designs, installs, drafts procedures for, or operates such systems.

What Is Management Consulting?

IIA Attribute Standard 1000.C1 states that the nature of consulting services must be defined in the charter. But just what is the nature of this work? After considering several different definitions, Milan Kubr came up with the following: 'Management consulting is an independent professional advisory service assisting managers and organisations to achieve organisational purposes and objectives by solving management and business problems, identifying and seizing new opportunities, enhancing learning and implementing changes.'[5]

The Institute of Management Consultants (IMC) has prepared a code of conduct that is binding on its members and which is based on three key principles of:

1. meeting the client's requirements;
2. integrity, independence, objectivity;
3. responsibility to the profession and to the IMC.

Moreover members have to ensure that in publicizing work or making representations to a client, the information given:

- is factual and relevant;
- is neither misleading nor unfair to others;
- is not otherwise discreditable to the profession.

In terms of adding value, we can return to Milan Kubr for a consideration of the two main aspects of consulting work being:

- The technical dimension, which concerns the nature of the management or business processes and problems faced by the client and the way in which these problems can be analysed and resolved.
- The human dimension, ie interpersonal relationships in the client organisation, people's feelings about the problem at hand and their interest in improving the current situation, and the interpersonal relationship between the consultant and the client.[6]

These two dimensions call for different types of tools, techniques and approaches. The auditor will probably be well versed in process-based problem solving, but may be on less sure ground when dealing with the human dimension. Even where the internal auditor is only concerned with, say, risk management systems, there is still a need to address the people issues when developing risk workshops, questionnaires or awareness seminars, and also ensuring that any new systems (or better focused systems) do not throw existing processes out of balance, which in practice tends to come full circle, back to issues of interpersonal relationships. The question of independence is also more complicated than at first sight. It may be thought that consulting work is never independent because the primary consideration is the interests of the client. But there is also the need to retain integrity, independence and objectivity in meeting these requirements. Milan Kubr has a view on independence that incorporates the following considerations:

> Independence is a salient feature of consulting. A consultant must be in a position to make unbiased assessment of any situation, tell the truth, and recommend frankly and objectively what the client organisation needs to do without having any second thoughts on how this might affect the consultant's own interests. This detachment of the consultant has many facets and can be a tricky matter in certain cases.

Consulting Work

The IIA sees a crossover between consulting work and the assurance role, which is unique to the audit position where strict confidentiality may not be an absolute. Performance Standard 2120.C2 makes it clear that 'Internal auditors must incorporate knowledge of risks gained from consulting engagements into their evaluation of the organization's risk management processes'.

One further point to note is that the internal auditor should not take on projects that cannot be undertaken competently. Attribute Standard 1210 says on this matter:

> Internal auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively must possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities.
>
> The CAE should decline the consulting engagement or obtain competent advice and assistance if the internal audit staff lacks the knowledge, skills or other competencies needed to perform all or part of the engagement.

Standards apply to consulting work as well as the more traditional assurance-based auditing. One point made by the guidance is that documentation used on assurance work may not be appropriate to consulting tasks and there are different techniques that may be applied, in particular to address the human dimension of consulting projects. There is some crossover between assurance and consulting work and one standard (2220.A2) suggests that:

> If significant consulting opportunities arise during an assurance engagement, a specific written understanding as to the objectives, scope, respective responsibilities, and other expectations should be reached and the results of the consulting engagement communicated in accordance with consulting standards.

Formal consulting projects are dealt with in Chapter 7 on audit approaches.

6.5 The Quality Concept

The IIA's Attribute Standard 1300 (Quality Assurance and Improvement Programme) states that:

> **1300 – Quality Assurance and Improvement Program**
>
> The chief audit executive must develop and maintain a quality assurance and improvement program that covers all aspects of the internal audit activity.

There is a lot being said about quality assurance, as this appears to be one of the standard management buzzwords. Quality is about the following:

- Knowing your business
- Knowing your customers and understanding how they see your business
- Looking for and dealing with problems
- Having a way of finding out what stakeholders think of the service
- Relating all problems to systems that need to be improved. In other words risks to success should be identified, assessed and managed
- Being very concerned about the section's reputation and overall standing in the organization

- A clear focus on value for money
- Resourcing the drive for quality
- Having efficient and effective procedures
- Having the quality role built into all staff and ensuring audit managers review and supervise work with this in mind
- Developing assessment models that can be used to judge whether quality standards are being met
- Adopting a culture of getting things right and continually improving

Several Attribute Standards address the quality concept:

1310 – The quality assurance and improvement program must include both internal and external assessments.

1311 – Internal assessments must include:

- Ongoing monitoring of the performance of the internal audit activity; and
- Periodic reviews performed through self-assessment or by other persons within the organization with sufficient knowledge of internal audit practices.

Periodic reviews are assessments conducted to evaluate conformance with the Definition of Internal Auditing, the Code of Ethics, and the Standards.

Sufficient knowledge of internal audit practices requires at least an understanding of all elements of the International Professional Practices Framework.

1312 – External assessments must be conducted at least once every five years by a qualified, independent reviewer or review team from outside the organization. The chief audit executive must discuss with the board:

- The need for more frequent external assessments; and
- The qualifications and independence of the external reviewer or review team, including any potential conflict of interest.

1320 – The chief audit executive must communicate the results of the quality assurance and improvement program to senior management and the board.

1321 – The chief audit executive may state that the internal audit activity conforms with the International Standards for the Professional Practice of Internal Auditing only if the results of the quality assurance and improvement program support this statement.

1322 – When nonconformance with the Definition of Internal Auditing, the Code of Ethics, or the Standards impacts the overall scope or operation of the internal audit activity, the chief audit executive must disclose the nonconformance and the impact to senior management and the board.

The Quality Equation

Without going into great detail, the key point that emerges from the latest research is that checking done at the end of a system (i.e. an operation) is an inefficient way of promoting quality. What is more relevant is to ensure that the systems themselves are steeped in a culture of quality from start to finish. This concept is, in truth, not new as it should underpin the whole thrust of internal audit's efforts in promoting better systems and systems controls. Nonetheless, internal audit like any other activity must set and meet quality standards under the direction of the CAE. The other feature of the drive towards quality assurance is the principle of getting the client to set these quality standards, as the ultimate recipient of audit services. One might argue that the CAE

is primarily responsible for quality assurance and procedures, and all the resources that should be directed towards the various related initiatives.

Poor Products

One key benefit from quality assurance is that poor working practices are seen in a different light. A poor audit report is not simply a matter of blaming the authors and bearing down on them. Substandard work becomes part of the learning process, where management seeks to address the underlying causes with a view to rectifying poor performance. Because audit work is primarily HR intensive, problems can normally be traced back to poor policies and procedures. However, in limited cases there can be other causes relating to, say, outdated information technology or a lack of facilities or demotivated staff. Again we return to the view that the CAE is responsible for all audit work and it is only through clearly thought-out procedures that this role can be fully accepted. Quality depends on a formal method of identifying poor products that relates problems back to systems. One has heard of the chef who never cooks at home and this image may run parallel to the auditor who never assesses risks and reviews their own systems of internal control. In truth there is no excuse for this stance, as in the long run it will impair the integrity of the internal audit function. Poor audits result from poor systems so long as we use systems in their widest form to include all those activities that are carried out to achieve business objectives.

Barriers and Constraints

Effective QA does not come about without much work and commitment. There are many barriers and constraints that act against the successful implementation of formal quality systems and these can represent major obstacles. Quality is a concept while quality assurance is a collection of well-planned management systems that take time and effort to apply. Some of the barriers to good quality include:

1. A failure by audit management to recognize (and/or understand) the importance of quality assurance systems. Quality systems have to be driven from above and they will not take effect if the required regimes do not attach to audit management as part of the commitment to good services. Where QA has been assimilated into management practices we are well on the road to a successful audit service.
2. Poor management information system that fails to provide feedback on performance targets. QA thrives on information since standards once established must be used to measure the efficiency of operations and services. Suitable information systems should be designed to spot defects. Proper QA systems are based on guiding the way resources are employed so as to minimize the incidence of any defects.
3. A redundant audit manual that is not able to act as the vehicle for defining and using audit procedures. A quality manual is required to set the frame for QA as a way of defining formal procedures.Where this is not in place we need first to set a change in the audit culture before the required documentation can be installed.
4. Internal audit departments that have failed to adopt good change management techniques which means that new procedures become very difficult to install. Serious QA programmes tackle the actual foundation of audit work by requiring a position of excellence wherever possible. This may depend on total quality management policies being adopted so as to provide a clear impetus to the search for quality.

5. An absence of formal audit strategy leading to a lack of direction. Quality systems will have to be attached to the current strategy to be of any real use, and where this does not exist, little or nothing will be achieved over and above mere statements of intent.
6. An absence of HR management practices, such as formal training programmes, leaving staff to 'sink or swim'. Management cannot insist on quality if they have not established support systems to underpin this venture. In this way there is a meeting of both sides where auditors and audit management both express a commitment to quality services.
7. A failure to appreciate the need for client-based systems that enable service recipients to specify their needs and expectations in respect of internal audit services. The reconciliation of independence and client needs should be undertaken with due regard to the need to formulate a model of audit service that duly takes on board both factors.

QA consolidates and stimulates the formal auditing procedures that underpin quality initiatives. A further concept that sits with the quality approach is one of continual improvement. This results from the feedback loops that are essential, where we seek to discover why things go wrong, with a view to putting right any controllable problems. Again, there is no excuse for auditors not being in tune with the view that management must be about a constant drive for improvements to systems and controls that impact on performance. Internal audit management must be fully conversant with the practice as shown in Figure 6.5.

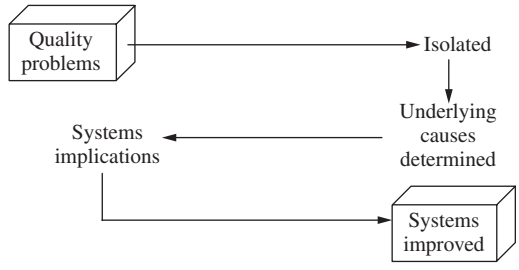


FIGURE 6.5 Quality and systems.

This may be seen as the single most important benefit of good quality practices.

The Appropriate Approach

One perplexing question that should come to the fore through quality assurance systems is that relating to the type of audit services that are being provided. Poor performance should not be confused with inappropriate audit services. Quality starts with asking the client for their view of the type of services that are required. This model is correctly applied to the vast majority of support services within an organization. There is a problem, however, for internal audit where we cannot always simply provide what management wants. There are times when we have to deliver a professional audit service, based on assessing business risks and management's control systems and then criticizing them where necessary. This may not be precisely what managers want particularly where they are insecure and have not properly resourced relevant control issues. Where the client is defined as the audit committee, rather than management *per se*, we move closer to an acceptable platform upon which to build quality systems. We must still ask whether the services that are provided by internal audit are suitable and match the organization's

control needs. Quality assurance should enable us to assess, reassess and further assess our audit services on an ongoing basis. So long as we have defined our client this assessment process should enable us to preserve the audit service as a long-term resource that is respected throughout the organization. Sawyer has described one approach by the auditor aimed at being fair and open to the client:

> This I will do for you: You'll be the first to know. We'll discuss it in whatever depth you wish. We'll present you with all the evidence we gathered. If you like, we'll show you our working papers. We'll search together for the causes. We'll explore together the effect, both actual and potential. I'll offer my counsel, based on my experience, on how to correct the difficulty and solve the problem. The corrective action will, of course, be yours, not mine. If I receive evidence of action taken or action begun with a due date for completion, I will stress that to your superiors and I certainly will not exaggerate the matter in my report. Can I be fairer than that, and still do my job?[7]

Appropriate Structures

Once we have determined the 'right' audit services we must reappraise the resources that are used to discharge the audit role. One of the main considerations is the type of structure that is adopted. In practice, many quality problems concerning the final audit product may be traced back to inappropriate structures where there is a mismatch between the required audit services and the way the audit function is organized. The key to defining an appropriate structure is to build this around the strategic question: What type of service is being aimed at and what quality standards are applied?

Compliance with Code of Conduct and Standards

One further point to note in respect of QA is the due reliance that is placed on professional standards. Quality systems must, above all, be able to distinguish non-compliance with professional standards, be they personal (i.e. relating to conduct) or operational. We would look to our systems to tell us whether internal audit is meeting the requirements of these standards. This entails the following:

1. Adopt suitable professional standards (e.g. IIA) as part of the formal mission statement that drives and directs the audit service.
2. Redefine the above as local standards via suitable enclosures in the audit manual. This creates an assimilation of outline standards into working practices as a necessary step towards fully integrating them into the audit role.
3. Implement them via a formal procedure whereby staff are advised as to the requirements of these standards and so understand all that this entails.
4. Train and develop staff to meet them.
5. Review compliance with standards via suitable control mechanisms.
6. Deal with any non-compliance as high-profile serious issues.
7. Review these standards to ensure that they make sense and fit with the audit work that is performed.
8. Seek to relate quality problems with these standards in terms of gaps therein or non-compliance. This is in full recognition of the systems approach to problem solving where all operational defects are related to deficiencies in the underlying systems.

Supervision

Auditors should be able to discharge their audit role in a professional manner and audit management will supervise this work in an appropriate manner. IIA Performance Standard 2340 (Engagement Supervision) states that:

> Engagements must be properly supervised to ensure objectives are achieved, quality is assured, and staff is developed.

The interpretation of this standard clarifies the requirement:

> The extent of supervision required will depend on the proficiency and experience of internal auditors and the complexity of the engagement. The chief audit executive has overall responsibility for supervising the engagement, whether performed by or for the internal audit activity, but may designate appropriately experienced members of the internal audit activity to perform the review. Appropriate evidence of supervision is documented and retained.

Supervision checks for compliance with agreed standards and procedures, while the other factor is that they should be provided with sufficient guidance and advice from audit management including clear terms of reference and any assistance where required. The team leader, audit manager and CAE each have a duty to ensure that they are available to direct staff as the audit is being conducted. The IIA Practice Advisory 2340-1 (Engagement Supervision) includes the following matters (extracts only):

1. The chief audit executive (CAE) or designee provides appropriate engagement supervision. Supervision is a process that begins with planning and continues throughout the engagement. The process includes:
   - Ensuring designated auditors collectively possess the required knowledge, skills, and other competencies to perform the engagement.
   - Providing appropriate instructions during the planning of the engagement and approving the engagement program.
   - Ensuring the approved engagement program is completed unless changes are justified and authorized.
   - Determining engagement working papers adequately support engagement observations, conclusions, and recommendations.
   - Ensuring engagement communications are accurate, objective, clear, concise, constructive, and timely.
   - Ensuring engagement objectives are met.
   - Providing opportunities for developing internal auditors' knowledge, skills, and other competencies.

   The CAE is responsible for all internal audit engagements, whether performed by or for the internal audit activity, and all significant professional judgments made throughout the engagement. The CAE also adopts suitable means to ensure this responsibility is met. Suitable means include policies and procedures designed to:
   - Minimize the risk that internal auditors or others performing work for the internal audit activity make professional judgments or take other actions that are inconsistent with the CAE's professional judgment such that the engagement is impacted adversely.
   - Resolve differences in professional judgment between the CAE and internal audit staff over significant issues relating to the engagement. Such means may include discussion of pertinent facts, further inquiry or research, and documentation and disposition of

the differing viewpoints in engagement working papers. In instances of a difference in professional judgment over an ethical issue, suitable means may include referral of the issue to those individuals in the organization having responsibility over ethical matters.

- All engagement working papers are reviewed to ensure they support engagement communications and necessary audit procedures are performed. Evidence of supervisory review consists of the reviewer initialing and dating each working paper after it is reviewed. Other techniques that provide evidence of supervisory review include completing an engagement working paper review checklist; preparing a memorandum specifying the nature, extent, and results of the review; or evaluating and accepting reviews within the working paper software.

Reviewers can make a written record (i.e., review notes) of questions arising from the review process. When clearing review notes, care needs to be taken to ensure working papers provide adequate evidence that questions raised during the review are resolved. Alternatives with respect to disposition of review notes are as follow:

- Retain the review notes as a record of the reviewer's questions raised, the steps taken in their resolution, and the results of those steps.
- Discard the review notes after the questions raised are resolved and the appropriate engagement working papers are amended to provide the information requested.
- Engagement supervision also allows for training and development of staff and performance evaluation.

Supervision is fundamental to audit management that seeks to isolate potential problems before they arise. This requires ongoing involvement of senior auditors in their staff's work, providing advice and guidance. A sure way of making this consistent and workable is to base the audit management input around the use of audit procedures, rather than ad-hoc tips. Larry Sawyer has made clear the importance of effective supervision:

> No mechanical control can compare with knowledgeable, accessible, concerned supervision. Professional, experienced auditors are likely to turn out professional audits; inexperienced auditors are not. Yet an audit department's products must be consistently high. The equalizer is good supervision. A competent supervisor can warn of pitfalls, help in the audit planning, provide unbiased perspectives on audit findings, ensure the preparation of professional working papers, help maintain good auditor–auditee relations, monitor budgets and schedules and help reverse adverse trends, review audit reports, and see that essential elements are not missing from the audit project.[8]

The audit review should be based around ensuring the auditor complied with procedures. These procedures play the key role when audit management is considering the quality of an audit. The reviewer must ask questions such as:

1. What were the procedures relevant to this audit? The answer will vary according to the type of work performed and the experience of the auditor in question.
2. Have these procedures been fully communicated to the auditor who carried out the work?
3. Is there sufficient evidence of compliance with these procedures?
4. Is there any evidence of non-compliance with these procedures?
5. Is there any explanation for apparent non-compliance?
6. Has the audit been a success, i.e. achieved its objectives? If this is not the case, do procedures, or the way they are used (or not used), need revising in any way?

We should try to move to a position where a cause-and-effect relationship is established, so that poor performance can be related to the underlying procedures that form the basis of audit work.

Link into Quality Assurance

In a previous section we discussed QA and agreed that it depends on clear and workable procedures. Much of the distinction is a matter of terminology since some of the available synonyms for the word 'procedure' include the following alternatives:

Action	Policy
Conduct	Practice
Course	Process
Custom	Routine scheme
Form	Step
Method	Strategy
Performance	System

The terms 'quality, standards and controls' also conjure up a similar picture as is painted by the use of the word 'procedures'. In one sense they are much the same way of describing the concept of formal management direction that is fundamental to the provision of QA. They are kept apart for convenience although the clear links must always be appreciated by audit managers.

Staff discipline A final point is the potential use of the concept of procedures in staff discipline, particularly where a formal disciplinary is being held against a member of the internal audit function department. In this instance, best practice concerning the use of procedures that have been breached should make them comply with several criteria before they may be used in a disciplinary:

1. Procedures must be clear and concise.
2. They must be fully communicated to staff.
3. Their status should be set out: whether they constitute instructions, rules, advice or explanations.
4. The people who are affected should be clearly identified along with any measures to deal with further information or guidance that may be required.
5. They should explain how compliance will be monitored and what are the staff's responsibilities in assisting this process.
6. The role of any warnings that will be given for instances of non-compliance.
7. The consequences of non-compliance must be defined, particularly where this is serious, e.g. a disciplinary and possible summary dismissal.
8. Important procedures should be reissued regularly and meetings used to convey their importance.
9. They may form part of the induction training for new starters.
10. Any non-compliance should be deliberate for it to have a role in a formal disciplinary.
11. They should be fair, consistently applied and meaningful.

Develop Quality Audit Staff

Quality is achieved through retaining good people. To ascertain what makes a good strategy, we can turn to an informal poll conducted by Jonathan Figg regarding successful strategies for finding and retaining the best workers, summarized below:

1. Pursue diversity – broaden the scope of recruiting efforts for a wider pool of talent.
2. Assess individual values – the right personality and values that match the organizations.
3. Be the best – good company images will attract good people.
4. Equip for success – make cutting edge technology available to staff.
5. Let go of the reins – empowerment continues to be an important element of successful staffing.
6. Remember the individual – balance work–life demands by being flexible and encouraging each person to grow as an individual.
7. Advance the people – encourage movement outside the internal audit shop to help motivate staff.
8. Recognize success – reward and recognition systems and positive exit interviews.
9. Develop the talent – training and development and management trainees having a spell in internal audit.
10. Talk it up – keep communication lines open say at monthly staff meetings.
11. Rewrite the book – review recruitment strategies to beat the competition for talent.[9]

The Vital Need For Quality Internal Auditing

By Dan Swanson *Compliance Week Columnist*

In the past few years, massive efforts have been expended to prepare and implement the requirements of the Sarbanes-Oxley Act, in particular Section 404. While a corporation's management and board of directors have always been responsible for internal control, the level of scrutiny by the investing public and the regulatory bodies has reached new levels. As a result, today more than ever before an organization's internal audit function must be robust and contribute to ensuring the accuracy of financial reporting. There's no question that fostering a strong internal audit department should be a high priority for management. Indeed, the Institute for Internal Auditors spells out as much in its International Standards for the Professional Practice of Internal Auditing: ''The chief audit executive should develop and maintain a quality assurance and improvement program that covers all aspects of the internal audit activity and continuously monitors its effectiveness.''

Fundamentally, internal audit efforts are focused on identifying the key goals, issues and challenges facing an organization and evaluating its progress. Internal auditors also assess senior management's procedures and related controls for achieving those objectives, while identifying opportunities for improvement. Each organization has different goals and objectives, and certainly specific issues and challenges facing a company depend on the business environment involved. Therefore, unfortunately, there is no one-size-fits-all internal audit process, nor one audit approach that fits all situations. But companies can ask themselves a few basic questions about what sort of internal audit function they want, and take steps to ensure the internal auditing they do meets those expectations. Start by defining the function. Internal audit provides

strategic, operational and tactical value to an organization's operations. For example, internal auditing is:

- A resource to the board and management for ensuring the entire organization has the resources, systems, and processes for operating an efficient and effective operation.
- An assurance tool for management and the board to know all that should be done is being done. By ensuring qualified professional reviews and tests are performed, the board and management can advance the goal of overseeing the organization's operations and ensuring its continuous improvement and success.
- An independent validation that the organization's efforts are proactive and effective against current and emerging threats.
- Some key questions the audit committee should be asking management:
- Has a quality assurance and improvement program within internal audit been established? What are the results to date?
- How do we know the internal audit function is effective? What are the key performance measures and results to date?
- How is the internal audit function doing in relation to the International Standards for the Practice of Internal Auditing? What are the strengths and weaknesses?
- Will the company meet the IIA's reporting deadline for reporting the external quality assessment review?
- Has the internal audit department begun its journey in quality?

Enter Quality Assurance

Professionalism does not occur overnight; it takes time. Professionalism evolves from dedication, professional growth and staff effort. Integral to this process – and the essence of excellence in the business environment – is quality. To ensure consistent quality in your internal audit function, a quality assurance and improvement program is necessary. The required elements include ongoing and periodic internal quality assessments, external quality assessments, internal monitoring, and assurance that the internal audit activity is complying with the IIA Standards and the IIA Code of Ethics. An external quality assessment, or QA, evaluates compliance with the Standards, the internal audit and audit committee charters, the organization's risk and control assessment, and the use of best practices. Regardless of an organization's industry or the internal audit team's complexity or size, two approved approaches to external QA are at the company's disposal. The first approach, an external assessment with independent validation, involves an outside team under the leadership of an experienced and professional project manager. The team members should be competent professionals who are well-versed in best internal audit practices.

The second approach seeks out an objective outside party for independent validation of an internal self-assessment and report completed by the internal audit group. This approach brings in a competent, independent evaluator experienced in quality assessment methodology to validate the aforementioned self-assessment of the internal audit activity. In addition to reviewing the self-assessment, the validator substantiates some of the work done by the self-assessment team, makes an on-site visit, interviews senior management, and either co-signs the chief audit executive's

report regarding conformity to the Standards or issues a separate report on the disparities.

The external quality assessment provides the audit committee and management with an official ''report card'' on the internal audit department's efforts and identifies opportunities for improvement. An effective internal audit function understands the organization, its culture, operations and risk profile. This makes audit a valuable resource for management, the board and its designated audit committee. The objectivity, skills, and knowledge of competent internal auditors can significantly add value to an organization's internal control, risk management, and governance processes. Similarly, effective internal audit can provide assurance to other stakeholders such as regulators, employees, investors, external auditors and shareholders. Completing the external quality assessment provides assurance to the audit committee and the board that internal audit is doing all the things it should be doing. And in today's climate of enhanced attention to financial reporting – a climate not likely to change any time soon – that robust internal audit function can only strengthen corporate performance.

6.6 Defining the Client

Professionalism and quality is about giving the client what they both want and need. This simple concept becomes more involved for internal auditors because we have several different stakeholders and because we deliver both assurance and consulting services. In the past, people who received audit services were simply known as auditees. However, we have moved on from here and there are various views on exactly how we deliver the audit service. The first point is that internal audit has moved away from a 'them and us' battleground as made crystal clear by many commentators:

> Abbey National's new chief internal auditor tells Neil Hodge what he thinks makes an invaluable audit function . . . 'Internal audit needs to make sure that it works as a kind of "controls consultant". It is definitely not tenable for internal audit just to sit back and pull management plans apart, however justified their criticism might be. Auditors need to work with management – not against it – and this needs to be made explicit in internal audit's dealings with the board . . . .'[10]

The internal auditor helps management get to grips with risk and controls while also telling the board and audit committee whether they can rely on the system for managing risk. The dual reporting aspects of internal audit have been summed up by Andrew Chambers:

> Primarily internal audit is a service for management, but to an extent internal audit also is an audit of management when it reports to the audit committee of the board. Since as far back as 1978 the Worldwide Standards for Internal Auditing have referred to internal audit as 'serving the organisation', not just serving management and certainly not just serving the accounting and finance functions.[11]

Getting to grips with the customer has been a concern of many CAEs as they develop their audit strategy:

> Internal audit customers . . . our first objective was to identify the individuals and entities to whom we provide a service. The more our audit staff discussed and debated, the more we came to realize that audit's customers exist throughout the organization and, in a few cases,

> outside it. Everything we do is ultimately for the benefit of Berkshire Life policyholders . . . Our final expanded list of direct customers included:
>
> - the president and board of directors
> - corporate officers and general agents
> - supervisors
> - non-supervisory employees
> - audit departments coworkers
> - external constituents such as CPSs and state examiners
>
> Once we understood and accepted the fact that internal auditing's customers included virtually everyone in the organization, we were prepared to initiate a survey process that would help us learn how well we were serving these customers. We determined that our audit process could be reduced to five basic categories that would be relevant to our customers:
>
> - audit planning
> - performance of audits
> - the reporting of results
> - our response to ad hoc requests for assistance
> - auditor professionalism.[12]

A very detailed consideration of the dual dimensions of auditing (assurance and consulting) has been made by Kenneth L Glascock which brings out the complexities of the quite unique experiences of internal auditors.

> In recent years, the term 'auditee' has fallen out of favor. Instead, those who receive audit services are now typically referred to as 'clients'. In this post-Enron era, when society is re-examining the value external auditors add in maintaining efficient capital, it is more important than ever for external and internal auditors alike to distinguish an auditee from a client . . . Although the term 'clients' has been widely adopted throughout the profession, I believe it is misused and highly problematic if applied in the context of assurance or traditional audit services. Referring to recipients of non-consulting services in this way implies a lack of objectivity, and it seems to contradict our professional obligation to remain independent. To clarify our role, we need to change the terminology used to describe those who receive audit or assurance services. The term 'auditees,' though shunned by many thought leaders in the profession, is a much more appropriate designation. Furthermore, the term is objective, neutral, and descriptive. Labeling those whom we audit in this manner does not imply that we should address them as auditees in person or in written reports. Instead, the term can be reserved for use among auditors, the audit committee, and management.[13]

6.7 Internal Review and External Review

Quality can be promoted by clear standards and effective supervision to ensure these standards are understood and employed throughout the audit shop. The CAE should also install a system of internal assessment to review whether everything is as it should be. The IIA's Attribute Standard 1311 requires the CAE to provide an internal assessment which should include:

- Ongoing monitoring of the performance of the internal audit activity; and

- Periodic reviews performed through self-assessment or by other persons within the organization with sufficient knowledge of internal audit practices.

The interpretation of this standard says that:

> Ongoing monitoring is an integral part of the day-to-day supervision, review, and measurement of the internal audit activity. Ongoing monitoring is incorporated into the routine policies and practices used to manage the internal audit activity and uses processes, tools, and information considered necessary to evaluate conformance with the Definition of Internal Auditing, the Code of Ethics, and the Standards. Periodic reviews are assessments conducted to evaluate conformance with the Definition of Internal Auditing, the Code of Ethics, and the Standards. Sufficient knowledge of internal audit practices requires at least an understanding of all elements of the International Professional Practices Framework.

Internal reviews may operate at a number of levels including reviewing the working papers and draft audit reports. One should develop a programme of audit reviews where audit management will carry out comprehensive reviews of, say, the bigger audits that have been completed. Spot checks may be undertaken at random on various audits to establish whether they are meeting acceptable standards. It is advisable to appoint one manager responsible for QA throughout the audit department. This person will report periodically (say annually) to the CAE on the overall position and indicate whether any changes to current practices are required. The internal review will consider various aspects of an audit that has been recently completed which includes:

- The source – how it came to be conducted.
- The preliminary survey and the way the terms of reference were established.
- The way the audit resources were assigned to the audit.
- The structure of the audit and whether it followed a logical approach to meet the set terms of reference.
- The way the documentation was put together and whether this was enough to meet the audit terms of reference but not excessive. The same reasoning applies to any testing carried out.
- The way the findings were gathered and placed into the report.
- The actual communication of findings and recommendations.
- The overall quality of the audit.
- Time management, budgets and the way audit hours were charged and accounted for.
- The extent of supervision and review and whether any potential and actual problems were dealt with.
- Whether the audit team demonstrated a good understanding of the audit standards in use.
- The extent to which the audit added value to the operation in question.
- The contribution the audit made to the annual assurance on internal controls provided by the CAE.
- Other considerations that impact on the quality of the audit.

The internal reviewer may also consider some of the wider issues, such as the risk-based planning procedures, use of tools such as CRSA, automated recording, performance management system, audit committee reporting. These issues may be difficult to address for people working within the audit shop as they will be too close to the action, and may be better addressed by the more wide-ranging external reviews. Internal reviews will tend to look at compliance issues with perhaps the occasional extra topic such as reviewing the time recording system in use or the

extent to which automated data interrogation is applied or whether we can let people work at home at times.

External Review

The IIA's Attribute Standard 1312 deals with external assessments:

> External assessments must be conducted at least once every five years by a qualified, independent reviewer or review team from outside the organization. The chief audit executive must discuss with the board:
>
> - The need for more frequent external assessments; and
> - The qualifications and independence of the external reviewer or review team, including any potential conflict of interest.

This is interpreted as follows:

> A qualified reviewer or review team consists of individuals who are competent in the professional practice of internal auditing and the external assessment process. The evaluation of the competency of the reviewer and review team is a judgment that considers the professional internal audit experience and professional credentials of the individuals selected to perform the review. The evaluation of qualifications also considers the size and complexity of the organizations that the reviewers have been associated with in relation to the organization for which the internal audit activity is being assessed, as well as the need for particular sector, industry, or technical knowledge. An independent reviewer or review team means not having either a real or an apparent conflict of interest and not being a part of, or under the control of, the organization to which the internal audit activity belongs.

External assessments, such as QA reviews, should be conducted at least once every five years by a qualified, independent reviewer or review team from outside the organization. There are various options for commissioning this wide-ranging review:

External audit – Here an overemphasis on financial systems and support for the external audit role may bias the work.

Internal audit departments in groups of companies – An informal policy of not criticizing each other may invalidate the work. Or fierce competition may make the review less than objective.

Reciprocal arrangements – Here companies may review each other, although confidentiality may be a real problem.

Other external auditors – Using other companies' external auditors helps reduce bias but they would still tend to have a financial orientation.

Consultant – A consultant who specializes in internal audit reviews will probably be the best choice in terms of skills, independence and final result.

The CAE should use the results of the external review to help form a strategy for improving the audit function and producing an effective quality programme. We can use the model in Figure 6.6 to illustrate the more traditional view of quality which starts at the end of the management cycle,

i.e. at the end of the audit. The issues that arise as a result of the QA process are then fed into the strategic analysis, and staff development exercises whereby any problems may be resolved. An alternative way of dealing with quality is to try to ensure that these problems do not arise in the first place, by establishing sound management and operational practices within the entire audit function. We have explained the three-point procedure of supervision, internal review and the occasional external reviews that feed into the quality process. The QA programme should be built into the strategic development process as a high profile item. In turn the strategy should then ensure that quality impacts directly onto staff development programmes in recognition of the far-reaching effects of moves in this direction as illustrated in Figure 6.6.

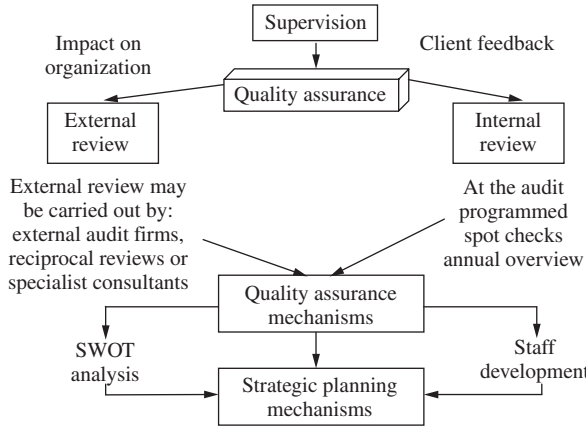


FIGURE 6.6 An audit quality assurance programme.

Practice Advisory 1312-1 provides guidance on these external assessments and extracts from this advisory are provided below:

> External assessments cover the entire spectrum of audit and consulting work performed by the internal audit activity and should not be limited to assessing its quality assurance and improvement program. To achieve optimum benefits from an external assessment, the scope of work should include benchmarking, identification, and reporting of leading practices that could assist the internal audit activity in becoming more efficient and/or effective. This can be accomplished through either a full external assessment by a qualified, independent external reviewer or review team or a comprehensive internal self-assessment with independent validation by a qualified, independent external reviewer or review team. Nonetheless, the chief audit executive (CAE) is to ensure the scope clearly states the expected deliverables of the external assessment in each case.
>
> External assessments of an internal audit activity contain an expressed opinion as to the entire spectrum of assurance and consulting work performed (or that should have been performed based on the internal audit charter) by the internal audit activity, including its conformance with the Definition of Internal Auditing, the Code of Ethics, and the Standards and, as appropriate, includes recommendations for improvement. Apart from conformance with the Definition of Internal Auditing, the Code of Ethics, and the Standards, the scope of the assessment is adjusted at the discretion of the CAE, senior management, or the board. These assessments can have considerable value to the CAE and other members of the internal audit activity, especially when benchmarking and best practices are shared. On completion of the review, a formal communication is to be given to senior management and the board.

> There are two approaches to external assessments. The first approach is a full external assessment conducted by a qualified, independent external reviewer or review team. This approach involves an outside team of competent professionals under the leadership of an experienced and professional project manager. The second approach involves the use of a qualified, independent external reviewer or review team to conduct an independent validation of the internal self-assessment and a report completed by the internal audit activity. Independent external reviewers should be well versed in leading internal audit practices.
>
> The CAE involves senior management and the board in determining the approach and selection of an external quality assessment provider.

The external review or assessment represents a chance for the audit management team to receive a report that gives a wide-ranging view on some of the key strategies and procedures. It also helps answer the question: Who audits the auditors? The reviewer will challenge some of the assumptions made by the internal audit shop and consider the extent to which it has embraced the risk management systems in terms of giving assurances and providing proactive help and assistance. The review will be concerned that audit is equipped to handle any heightened expectations from customers and stakeholders. One way of establishing the terms of reference for the review is to get the audit team together and carry out a formal risk assessment process and end up with a list of key risks and associated key controls that are being relied on. This information may be used to drive the review, in that it would seek to tackle the key risks and also consider how robust the key controls are. Stakeholders such as the audit committee and the main board can input into the draft terms of reference in an attempt to ensure that the resulting report has value. The review will look at whatever is set in the agreed terms of reference, which as suggested could come from a risk workshop. However, it may well include some of the following areas:

1. Audit charter – mission and vision and buy-in from staff and stakeholders.
2. Organizational status.
3. Independence.
4. Codes of conduct and internal disciplinary mechanisms.
5. Mix between assurance and consulting activity.
6. Audit strategy and whether it fits with corporate strategy of organization.
7. Relations with the board, senior manager and general reputation.
8. Interface with audit committee and whether best practice measures used to keep the audit committee informed.
9. Links with external audit and internal review teams.
10. Performance measurement system and whether this makes sense – also links with performance reporting systems.
11. Communications and participation between auditors and also with external parties – whether is used web-based material.
12. Mix of specialist areas such as fraud, IT, projects, contract and other.
13. Complaints procedure and whether this picks up all significant problems.
14. Structure and flexibility – in response to changes and strategies.
15. Staff competence, qualification and CPD.
16. Morale levels among auditors, and remuneration and retention rates – Why do people leave internal audit? Policies on secondment, career auditors and short-term placements.
17. Formal training programmes.
18. Research into developing best practice and links with professional bodies, local universities, conferences and international developments. Do the audit staff keep themselves up to date?

19. Planning systems and the annual audit plan.
20. Budgets and budgetary control, also cost per audit day.
21. Extent to which audit is accomplishing its objectives.
22. Planning and control of audit assignments and supervision arrangements.
23. Working papers, standards and compliance (also extent of automation, protection, security, retention, back-up and confidentiality).
24. Level of equipment such as laptops, communication links, etc.
25. Balance work–life issues and use of flexible approaches such as working from home.
26. Measures to encourage diversity among staff.
27. QA systems and whether internal reviews are adequate – the review will start with considering outcomes of recent internal reviews.
28. Due professional care and measures taken to ensure professionalism and consistency – including the use of the audit manual.
29. Compliance mechanisms to ensure laws and regulations are adhered to.
30. The adopted value add proposition and whether this is being achieved.

The list is, in one sense, open ended – it really depends on the risks that form the basis of the terms of reference for the review. Where the three-pronged approach of supervision, internal and/or external review uncovers a problem to do with non-compliance, this problem needs to be addressed. The audit committee and senior official need to be informed where this impacts the overall scope or operation of internal audit, including a lack of external assessment. Meanwhile, the chief audit executive must communicate the results of the quality assurance and improvement programme to senior management and the board (IIA 1320 standard)

Best Value Reviews

Best value reviews are carried out on local government services by the Audit Commission and the services reviewed include internal auditing. The Accounts and Audit Regulations 1996 require local authorities to maintain an adequate and effective system of internal audit of their accounting records and control systems. To this end internal audit should appraise and review:

- the completeness, reliability and integrity of information, both financial and operational;
- the systems established to ensure compliance with policies, plans, procedures, laws and regulations;
- the means of safeguarding assets;
- the economy and efficiency with which resources are employed;
- whether operations are being carried out as planned and objectives and goals are being met.

The Audit Commission prepares reports following their inspections under section 10 of the Local Government Act 1999 to:

1. enable the public to see whether best value is being delivered;
2. enable an inspected body to see how well it is doing;
3. enable the Government to see how well its policies are working on the ground;
4. identify failing services where remedial action may be necessary;
5. identify and disseminate best practice.

The Audit Commission reviews of various internal audit functions are based on the CIPFA code on internal audit in conjunction with the best value criteria of:

1. Challenging – how the service is provided.
2. Comparing – the KPIs with other.
3. Competition – embrace fair competition as a means of becoming more efficient and effective.
4. Consulting – with local taxpayers, customers and the wider business community.

After having analysed some eight best value reviews carried out between November 2000 and November 2001, we have summarized the work carried out, assorted strengths, assorted weaknesses, scoring and assorted recommendation which are listed below:

1. **Work carried out:**
   - Review documents provided in advance – e.g. improvement plan.
   - Review – corporate finance business plan, audit strategic plan, annual audit plan, benchmarking club details, invitation to tender packs.
   - Review sample of ten audit reports selected per risk and materiality.
   - Contact recipients of these reports.
   - Review sample of working files.
   - Interviews with audit members and users.
   - 'Walking the floor' of the internal audit service.
   - Staffing structure.
   - Internal audit progress reports.
   - The risk assessment system.
   - Investment in People Assessment Reports.
   - Review of internal audit by external consultants.
   - CIPFA Code of Practice.
   - Following the audit process from start to finish.
   - Reviewing the website.
   - Internal audit training plan.
   - Reality checks – focus groups from internal audit and client groups.
2. **Assorted strengths:**
   - Strong reporting lines.
   - Effective anti-fraud service.
   - Local KPIs based on service outputs.
   - Good performance management system.
   - Considerable consultation with the private sector.
   - Significant member involvement.
3. **Assorted weaknesses:**
   - Lack of transparency in audit coverage.
   - No long-term vision/strategy that matches audit resources to local authority's top objectives.
   - Lack of balanced audit work – no computer audits.
   - Variable user satisfaction – e.g. audit reports took too long to arrive.
   - Performance management arrangements unable to enable comparisons between actual and standards.
   - No challenge element in improvement plan – unable to consider different ways to deliver services.
   - No formal mechanism for reporting to members.

- Failure to deliver the annual audit plan.
- Failed to cover fundamental systems for last three years.
- Procedures for monitoring progress of planned work have stopped.
- Approach and methodology do not accord with professional standards.
- No response to problem of long-term absences.
- No overall strategic leadership.
- Improvement plan does not address major problems.
- Poor relationships with clients and within the internal audit team.
- Audit service not high profile enough.
- Some audit activities lacked added value or benefits.
- No skills for computer or contract audit.
- Risk management techniques not yet developed.
- Inconsistent working practices between team members.
- No comprehensive strategic audit plan.
- Lack of priority in implementing audit recommendations.
- No evidence of added value from the audit service.
- Poor timing of audits – at the end not start of change processes.
- General perception that internal audit is very low profile.
- No action on some audit recommendations.
- User was able to detrimentally weaken an audit report.
- Focus unclear with no assessment of needs.
- Ineffective reporting lines.
- No CAE and only half of the audit complement in post.
- Failure to alert management about irregularities found during audits.

4. **Scoring:**
   - Whether currently a good service (poor, fair, good, excellent).
   - Whether likely to improve as things stand (no, unlikely, probably, yes).
5. **Assorted recommendations:**
   - Benchmark with top performers – cost per day, completion of audit plans, percentage recommendations accepted versus not accepted, percentage directly chargeable work, percentage clients satisfied, timeliness of reports.
   - Explore competitive options – e.g. partnerships with other providers.
   - Develop objectives relating to risk management and corporate governance.
   - Consolidate terms of reference into an audit charter.
   - Maximize use of IT.
   - Appoint a CAE.
   - Improve consultation with clients.
   - Develop a more overt link between the audit plan and budgets.
   - Fast-track a risk-based method for focusing audit resources.
   - Address the non-implementation of audit recommendations.
   - Create an audit committee.
   - Develop a risk-based strategic plan.
   - Review customer satisfaction.
   - Frauds reported to the audit panel.
   - Better definition of contracting-out arrangements.
   - Ensure achievement of annual plan.
   - Identify specific improvement targets.
   - Introduce specific performance indicators.

- Consider improving internal audit through external contracts.
- Fundamental re-examination of the role and internal audit.

The above gives a good insight into external reviews, how they are undertaken and the types of findings that are uncovered. Much is based on an assessment of risks and the controls (and wider risk management strategy) needed to ensure the service is successful.

6.8 Tools and Techniques

There are various methods an organization (or for that matter an internal audit shop) may adopt to check the quality systems against established standards. Some of the more popular UK-based approaches are noted below.

ISO 9000 Quality Management Systems (www.iso.ch)

This standard can be used by internal audit to install an accredited quality management system into the way the audit product is delivered. The ISO 9001:2000 standard can be used to measure the audit service against an established criterion where the quality system is externally certified. The standard has five main sections:

1. product realization
2. quality management system
3. management responsibility
4. resource management
5. measurement, analysis and improvement.

The internal audit unit will have to show how these sections were applied in the audit quality manual. Moreover, the quality standard is based on eight quality management principles that can be applied when setting up a quality management system:

Principle 1 **Customer focus:** Organizations depend on their customers and therefore should understand current and future customer needs, should meet customer requirements and strive to exceed customer expectations.

Principle 2 **Leadership:** Leaders establish unity of purpose and direction of the organization. They should create and maintain the internal environment in which people can become fully involved in achieving the organization's objectives.

Principle 3 **Involvement of people:** People at all levels are the essence of an organization and their full involvement enables their abilities to be used for the organization's benefit.

Principle 4 **Process approach:** A desired result is achieved more efficiently when activities and related resources are managed as a process.

Principle 5 **System approach to management:** Identifying, understanding and managing inter-related processes as a system contributes to the organization's effectiveness and efficiency in achieving its objectives.

Principle 6 **Continual improvement:** Continual improvement of the organization's overall performance should be a permanent objective of the organization.

Principle 7 **Factual approach to decision making:** Effective decisions are based on the analysis of data and information.

Principle 8 **Mutually beneficial supplier relationships:** An organization and its suppliers are interdependent and a mutually beneficial relationship enhances the ability of both to create value.

Charter Mark (www.chartermark.gov.uk)

This is a Government award scheme for recognizing and encouraging excellence in the public sector. Charter Mark performance areas:

1. **Set standards** – set clear standards of service that users can expect, and monitor and review performance and publish the results, following independent validation, wherever possible.
2. **Be open and provide full information** – be open and communicate clearly and effectively in plain language to help people using the service; and provide full information about services, their costs and how well they perform.
3. **Consult and involve** – consult and involve present and potential users of the service as well as those who work with you; and use their views to improve the service provided.
4. **Encourage access and the promotion of choice** – make the service easily available to everyone who needs it including using new technology to the full, offering choice wherever possible.
5. **Treat all fairly** – treat all people fairly, respect their privacy and dignity, be helpful and courteous and pay particular attention to those with special needs.
6. **Put things right when they go wrong** – put things right quickly and effectively; learn from complaints, have a well publicized and easy to use complaints procedure, with independent review wherever possible.
7. **Use resources effectively** – use resources effectively to provide best value for stakeholders, taxpayers and users.
8. **Innovate and improve** – always look for ways to improve the service and facilities offered, particularly the use of new technology.
9. **Work with other providers** – you work with other providers to ensure that the services are simple and easy to use, effective and co-ordinated, and deliver a better service to the user.
10. **Provide user satisfaction** – show that users are satisfied with the quality of service they are receiving.

This approach was used by Cheltenham Borough Council's Audit and Assurance to achieve the Charter Mark Award. Duncan Edwards and John Cummins explained that:

> Going through the Charter Mark application process has convinced us that the answer (is internal audit different?) is a resounding no. The way we interact with our customers should be no different from any other service. No matter what sector you operate in the Charter Mark process will be a very useful benchmark to test your performance against and to critically appraise the way you determine and deliver your service.[14]

Benchmarking against CFIA

Kurt F. Reding, Craig H. Barber and Kristine K. Digirolamo bring home the use of CFIA as a benchmark:

> Benchmarking against the CFIA Competency Standards was a thought-provoking and constructive process for us. We gained vision and insights that will help us to make informed decisions about the future direction of Allstate's internal audit function. We also identified specific process improvement opportunities and formulated strategies for pursuing those opportunities. In confronting our role with regard to consulting, appraisal, and assurance services, we felt we were dealing with unresolved areas. We're convinced that the development of professional standards by the IIA will help internal auditors around the world add value to their organizations and sharply advance the profession's conceptual framework.[15]

European Foundation Quality Model (www.european-quality.co.uk)

This international model recognizes the need to give people a better working environment and provide their customers with the best possible value and quality and was first introduced in 1992. The European Quality Award is open to high performing organization in Europe and provides independent feedback from appointed assessors to help organizations as they embrace the concept of excellence. Using information published by the EFQM (website: efqm.org), the concepts that underpin the EFQM are noted below:

- **Results Orientation:** Excellence is dependent upon balancing and satisfying the needs of all relevant stakeholders (this includes the people employed, customers, suppliers and society in general as well as those with financial interests in the organisation).
- **Customer Focus:** The customer is the final arbiter of product and service quality and customer loyalty, retention and market share gain are best optimised through a clear focus on the needs of current and potential customers.
- **Leadership & Constancy of Purpose:** The behaviour of an organisation's leaders creates a clarity and unity of purpose within the organisation and an environment in which the organisation and its people can excel.
- **Management by Processes & Facts:** Organisations perform more effectively when all inter-related activities are understood and systematically managed and decisions concerning current operations and planned improvements are made using reliable information that includes stakeholder perceptions.
- **People Development & Involvement:** The full potential of an organisation's people is best released through shared values and a culture of trust and empowerment, which encourages the involvement of everyone.
- **Continuous Learning, Innovation & Improvement:** Organisational performance is maximised when it is based on the management and sharing of knowledge within a culture of continuous learning, innovation and improvement.
- **Partnership Development:** An organisation works more effectively when it has mutually beneficial relationships, built on trust, sharing of knowledge and integration, with its Partners.
- **Public Responsibility:** The long-term interests of the organisation and its people are best served by adopting an ethical approach and exceeding the expectations and regulations of the community at large.

The EFQM award has four levels of recognition:

1. **Award Winner:** The European Quality Award is presented annually to the organisation judged to be the best in each of the Award categories providing also they meet all the requirements set annually by the Award jurors.
2. **Prize Winners:** Prizes are presented annually to organisations that excel in some of the fundamental concepts of Excellence.
3. **Finalists:** Each year, several Finalists may be declared in each category.
4. **Recognised for Excellence:** All Applicants for the Award are asked if they are interested in being recognised at this level which is the middle level of EFQM Levels of Excellence. Those who achieve a score in excess of 400 points after site visit are Recognised for Excellence. This indicates that the organisation is well managed and aspires to achieve role model status. Successful organisations receive a framed certificate and they are also entitled to use the Recognised for Excellence logo on letterheads, business cards and other correspondence.

The EFQM Excellence Model is a non-prescriptive framework based on nine criteria. Five of these are 'Enablers' and four are 'Results'. The 'Enabler' criteria covers what an organization does. The 'Results' criteria covers what an organization achieves. 'Results' are caused by 'Enablers' and feedback from 'Results' helps to improve 'Enablers'.

The model, which recognizes that there are many approaches to achieving sustainable excellence in all aspects of performance, is based on the premise that: '*Excellent results with respect to Performance, Customers, People and Society are achieved through Partnerships and Resources, and Processes.*'

Investors in People (www.IiPuk.co.uk)

Many people see the 'people' factor as the key to success, and all measures that focus on getting the right staff to do the right things need to be prioritized. While many quality models concentrate on processes, and see the employees as just one factor in the process, the Investors in People (IiP) standard emphasizes the human factor. The idea is that a better motivated and equipped workforce delivers better performance using the policy: 'Take care of your people and they will take care of your business'. The costs of taking care being worthwhile compared to the benefits of better business performance. IiP consists of a national standard that promotes the training and development of employees by organizations, in a drive to ensure continuous improvement in performance. The IiP standard has four main elements:

1. **Commitment** – from the top to develop all employees to achieve its business objectives:
   - There is a public commitment from the most senior level within the organization to develop people.
   - Employees at all levels are aware of the broad aims or vision of the organization.
   - There is a written but flexible plan which sets out business goals and targets.
   - The plan identifies broad development needs and specifies how they will be assessed and met.
   - The employer has considered which employees at all levels will contribute to the success of the organization and has communicated this effectively to them.

- Where representative structures exist, management communicates with employee representatives a vision of where the organization is going to and the contribution employees (and their representatives) will make to its success.

2. **Planning** – regularly reviews the training and development needs of all employees.
   - The written plan identifies the resources that will be used to meet training and development needs.
   - Training and development needs are regularly reviewed against business objectives.
   - A process exists for regularly reviewing the training and development needs of all employees.
   - Responsibility for developing people is clearly identified throughout the organization, starting at the top.
   - Managers are competent to carry out their responsibilities for developing people.
   - Targets and standards are set for developing actions.
   - Where appropriate, training targets are linked to achieving external standards and particularly National Vocational Qualifications (or Scottish Vocational Qualifications in Scotland) and units.
3. **Action** – takes action to train and develop individuals on recruitment and throughout their employment:
   - All new employees are introduced effectively to the organization and are given the training and development they need to do their job.
   - The skills of existing employees are developed in line with business objectives.
   - All employees are made aware of the development opportunities open to them.
   - All employees are encouraged to help identify and meet their job-related development needs.
   - Effective action takes place to achieve the training and development objectives of individuals and the organization.
   - Managers are actively involved in supporting employees to meet their training and development needs.
4. **Evaluation** – evaluates the investment in training and development and improves future effectiveness:
   - The organization evaluates how its development of people is contributing to business goals and targets.
   - The organization evaluates whether its development actions have achieved their objectives.
   - The outcomes of training and development are evaluated at individual, team and organizational levels.
   - Top management understands the broad costs and benefits of developing people.
   - The continuing commitment of top management to developing people is communicated to all employees.

Once an organization has got to grips with the IiP standard, it can develop HR processes that meet the above-mentioned areas. It will then undertake a self-diagnosis against the IiP's set standard and gather evidence to the extent to which it is able to meet the requirements, and address any shortcomings. The evidence compiled by the organization will then be verified by a local Training & Enterprise Council (TEC) and if the verification is successful the organization is awarded IiP status. Reviews are generally carried out every three years. Proponents of the standards argue that installing IiP into sections around an organization, including the internal audit shop, may lead to:

- shared sense of purpose;
- better understanding of role in achieving business objectives;

- involvement in business improvements;
- release staff potential;
- job satisfaction;
- customer satisfaction;
- public recognition.

Why Standards?

The internal audit department may wish to show that it had installed the required procedures and controls to meet the various quality standards mentioned above. In addition, these procedures would also be reviewed by external assessors before accreditation is achieved. There is an expense involved and registration is in no way mandatory. There may come a time, however, when we might question why audit has failed to secure such a status particularly where activities that are being audited have already been fully accredited. It clearly is a matter that should remain high on the agenda of audit management team meetings.

6.9 Marketing the Audit Role

The IIA distance learning manuals have made clear the need for internal audit to prove its position in an organization:

> In this day and age no function has the right to exist. Each must be able to demonstrate how it adds value to the organisation, and can expect to be continually questioned about its role and contribution. Although internal audit is primarily a review function it is increasingly coming under the same scrutiny as every other part of an organisation and must be able to justify its existence.[16]

Should Internal Audit Adopt a Marketing Profile?

There are those who argue that the unique feature of the internal audit function that relates to its independence in some way means that there is no need to adopt a market-based orientation in the way services are delivered. They may go on to suggest that if we let managers define the way internal audit works then we become little more than consultants. This view is misconceived as it fails to recognize that internal audit is a service to the organization and not to itself, although there are some considerations that impact on a purist view of marketing.

Revisiting the Acid Test

One useful way of assessing whether our marketing efforts have interfered with the levels of independence that we should have achieved is to apply the basic acid test:

> If internal audit were instantly removed from the organization, would certain operations collapse?

A purist's view would insist that this question receives a negative answer to reinforce the concept of the audit services being free from operational involvement. The dilemma, from a marketing

angle, is that this exposes the audit role and makes it akin to a dispensable commodity. This problem warrants further exploration since there is an inherent conflict between the marketing concept and the independence test that must be recognized and managed by the CAE.

Different Approaches to Marketing

We move to marketing as it impacts on the internal audit role. This may be set within an illustration of the marketing approach contrasted with other managerial standpoints as shown in Figure 6.7.

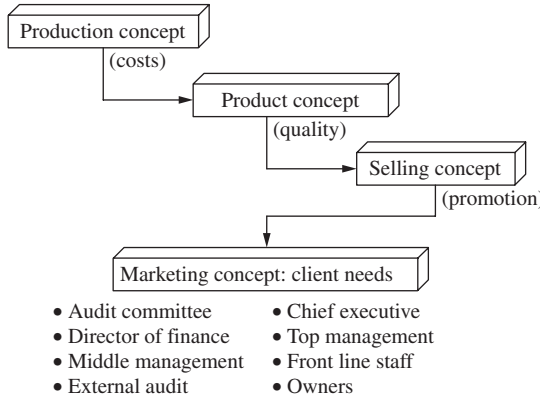


FIGURE 6.7 The marketing concept.

The IIA.UK&Ireland has suggested that audit clients fall into three groups: those it reports to (e.g. audit committee), those it reports on (e.g. middle management) and those it reports with (e.g. external audit and internal control teams). The **production concept** seeks to minimize the costs of the audit, which translates to the number of hours spent on each individual project. The **product concept** will on the other hand concentrate on the audit itself and suggests that so long as the work is good and the report is done to quality standards everything will be fine. The **selling concept** is particularly relevant to internal audit in that it suggests we need only ensure that the client pays for our services, which may be mandatory in most organizations who resource an audit function. The **marketing approach**, on the other hand, takes the view that we must first find out what is required by the organization and then seek to meet these requirements. No matter how efficient or professional the audit work is, so long as we have not fed our work into client expectations then our future is not assured. This may come as a surprise to many auditors who do not believe that they (or the CAE) work for anyone.

The Marketing Mix

Marketing audit services starts with being able to offer professional services. Services should be publicized and arrangements set out for first identifying and second addressing any concerns that clients may have with the quality and delivery of audit services. Marketing helps extend the audit role beyond the point where the final report is issued and brings home the undeniably important

concept of effective client-based service delivery. The following types of questions should be addressed via a carefully planned marketing strategy:

1. What kind of audit services should be provided?
2. What should be the balance of unplanned (response-based) work to planned audits?
3. How much time should be spent on consultancy projects as opposed to systems audits?
4. What should be the mix of senior/junior auditors?
5. Following on from the above, what level of hourly charge-out rate should be aimed at?
6. How do we promote the audit image?
7. Are our clients satisfied with the services that we are providing?
8. How are we placed *vis à vis* our potential competitors?

The product Here we consider whether the audit work that is being provided fits with the requirements of the organization. The Boston Box comes to our aid in making this consideration when deciding our product strategy. This may consist of doing nothing, seeking new developments, seeking market developments, diversification and/or going for new markets as shown in Figure 6.8.

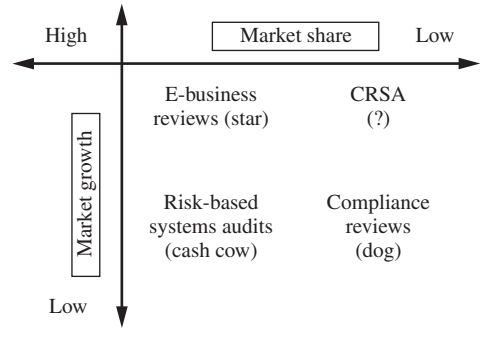


FIGURE 6.8 Boston Box – Assessing audit service.

We may aim at a balanced portfolio of audit work in line with the classifications of the Boston Box:

The price The costs of the audit work should be subject to ongoing review so as to work to an optimum profile. Different types of audit work take different time frames to complete and different types of auditor, some expensive (e.g. an information systems auditor) and others relatively cheap (e.g. a junior auditor). The starting place is to ensure that costing systems are sound and that they differentiate between different grades of auditor. Premium work that may have to be done on overtime or require additional consultants to be brought in will be charged at higher rates than standard audits.

Promotion This may be seen more as being built into the public relations function as a way of selling the audit image and underlying services. Where we have adopted a push strategy we will be seeking new fields of work and promoting the audit service. A formal complaints procedure will help identify the state of the audit image and it may be necessary to create defined messages to reinforce the profile of the audit service. The annual report is a useful vehicle for promoting the audit presence.

Audit Feedback Questionnaire

One way of achieving a degree of feedback from the client is to obtain a response to a formal questionnaire that makes enquiries about the audit service. We have already outlined the survey of clients as part of the QA programme and a major control that the CAE may use to assess the success of internal audit. The client survey also has a role in the marketing plan since it constitutes a formal mechanism for obtaining independent evidence of audit's successes and problems when dealing with clients. The survey has to be carefully administered since it should not give the impression that audit management does not trust its staff, neither should it be an opportunity for line managers to undermine the field auditors. Accordingly the purpose of the survey should be explained in a covering memo from the CAE and the main objectives are:

- to obtain the client's view on the benefits secured from the audit;
- to isolate any communication problems that may have been experienced by the client;
- to assess whether the client's perceived needs have been met;
- to identify any adjustments to marketing strategy and audit methodologies that may be required.

The client surveys operate at two levels: one as an assignment follow-up while the other looks for more general comments that are not linked to any particular audit. An Audit Effectiveness Questionnaire, along with a covering memorandum from the CAE, may be given to the client by the lead field auditor and once the audit has been completed it will be returned direct to the CAE. It is felt that allowing the field auditors to distribute and explain the survey dispels the view that the CAE does not trust them. The arrangement whereby the form is filled in by the client and returned direct to the CAE ensures that the client may be quite open in their views. Audit working papers will note any disagreement that the auditors may have had with the client and this point should be taken on board when reviewing the survey results. A wider survey may also be carried out from time to time, which can be used to provide feedback on audit's overall impact on management, for use in formulating audit marketing plans. The need to ensure internal audit remains relevant has been discussed by Barry S. Leithhead:

> The first step auditors must take toward ensuring their relevancy is to expand their focus to include the entire control system, not just control activities. Doing so requires auditors to consider all risks the organization may face. First, they must consider the current risks that need to be controlled and determine whether all components of the control-system design are adequate and effectively applied. Next, auditors should identify the possible future risks and determine whether the current control systems will manage these anticipated risks. Finally, the auditor should recognize which current and future risks may have the greatest impact on the organization. When auditors go through this process of expanding their thinking from control activities to future risks, then they can add true value to the organization.[17]

The Audit Website

This standing forum can be used to provide much of the detail that clients might require along with details of audit services and contact names. It should be a brief, colourful, foldable brochure possibly with several photographs. Reference can be made to the published annual report for more comprehensive information, on the basis that a brochure with excessive detail will tend not to be read. It is also advisable to have a brochure produced professionally from a print shop

where a glossy, conveniently sized pamphlet may be commissioned without appearing excessively flamboyant. It should be given to employees on those occasions when auditors feel this would be appropriate, covering:

- What is internal audit?
- What can internal audit do for you?
- Who do you contact?

The audit department should ideally follow a house style with an appropriate logo that projects the basic image that audit wishes to present. The audit name and logo will appear on all correspondence and reports, and a suitable 'house colour' will also be used for all published documents, including the brochure. We may go on to contact management where it requires further information on the internal audit services. The internal audit website may be structured in the following manner:

1. Introduction. General background to the audit role, audit standards and how work is undertaken. Independence, audit approach, fraud and other relevant issues can be briefly described.
2. Summary of year's achievements. The particularly major reviews will be mentioned along with the real benefits that accrued.
3. Available audit services. Here the main services will be set out and the type of control-related problems that can be solved.
4. The service level agreement. Audit plans, contingency work, special requests and the audit scheduling process will be outlined along with mention of the fee charging system. The complaints procedure may be defined which involves direct representation to the CAE.
5. Understanding internal controls. Management's responsibilities may be highlighted in this section which will discuss the general concept of control and ways that management may discharge its responsibilities in this matter.
6. Contacts. A brief list of the main contacts will be set out. The group structure and responsibility levels will be provided to ensure that management is able to contact the right audit manager wherever necessary.

Remember visitors may be regular customers or just casual enquirers and the website should be both attractive and informative. Frequently asked questions for website use are listed in Chapter 5, Section 5.8 of the Handbook.

Auditors' Business Cards

Each auditor may be issued with a business card that will set out:

- the auditor's name;
- the designation;
- any professional/academic titles;
- areas of responsibility;
- the contact phone number.

Again the audit logo would appear on this document.

A Complaints Procedure

A formal complaints procedure should be applied whereby management is advised of a clear process for submitting their concerns. The introductory memoranda to management may include the following paragraph:

> We hope that you will not experience any problems with the audit work since all auditors work to the highest professional standards. However, should you have any particular concern, please voice them to **x** who is the team leader for this project. In the event that you are still not satisfied please contact the CAE.

Marketing Information

Marketing decisions must be based on sufficient information and some of the main sources of this information are:

- General feedback from auditors on management's views. Here the CAE should have regular contact with senior management to discuss general audit-related matters.
- Level of complaints from clients.
- Formal responses from the audit committee.
- Results of the formal client survey.
- Surveys of competitors.
- Internal reports produced by the organization that mention internal audit.
- Feedback from auditors.
- Informal contacts with employees and people associated with the organization.

Each source provides an insight into the success or otherwise of the marketing plan and they need to be carefully monitored.

Marketing Plans

There is a link between marketing and audit strategy, and many strategic decisions will have an impact on the marketing plan. As a result, the strategic plan should also incorporate the marketing plan and revisions to strategy may well affect the way internal audit is marketed as shown in Figure 6.9.

These plans should be assimilated into audit strategies and form the basis of discussions at the audit manager meetings that should be held regularly. One audit marketing strategy uses seven key principles:

- to act as partners with management focusing on adding value while maintaining the necessary independence;
- to align the audit planning to the aims, objectives, risks and processes of the organization;
- to champion the continuous improvement of the systems of risk management internal control;
- to provide accurate and timely advice and assurance to management;
- to invest in quality staff, training and techniques;
- to be professional in everything we do;
- to provide a cost-effective and valued service.

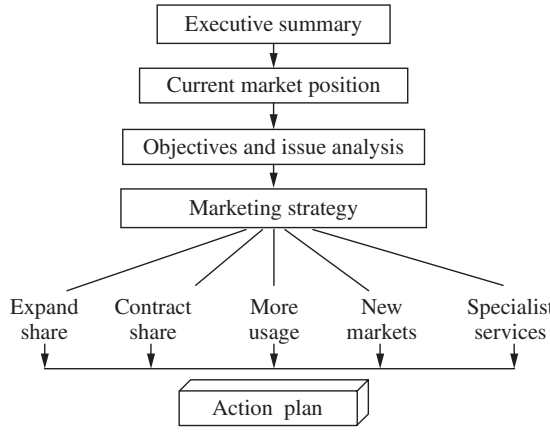


FIGURE 6.9 Marketing plan structure.

Analysis of Competitors

For many years the public sector has faced the threat of competition from external providers of audit services. There is a need for extensive preparation in this environment, since much of the drive is about allowing the in-house team to bid for the contract in competition with other suppliers. There are many examples of public sector audit functions that are now being performed by private sector firms. To this end an analysis of the current market can be a useful exercise and provide important information that can be fed into the marketing strategy. We would be concerned with:

- entry barriers that stop new suppliers entering the market for internal audit services;
- competitors' reactions to the contracts that may become available for competition and whether they have expressed an interest in submitting a bid;
- competitors' strengths and weaknesses in comparison to what may be provided by the existing audit unit.

It may be possible to develop a competitors' intelligence system or subscribe to a service that regularly provides this type of analysis. Essentially the results will provide an insight into the types of decisions (i.e. improvements) that are required to make the in-house service better placed than competitors' services.

Consumer Behaviour

It is as well to research the attitudes of clients and seek to understand their behaviour. Independence can be used to strengthen the audit role and ensure our reports are heard at the highest levels. If, however, we are not satisfying the needs of audit clients generally, we cannot simply hide behind the cloak of independence and ignore this factor. We should be concerned about clients' attitudes towards internal audit and how they use audit services. We need to pay particular attention to unsatisfied needs, and how these may be met through a revision to the service provision profiles that we have discussed above.

The Audit Budget

Clients pay for audit services through the quarterly fee charging system, and it is essential that the charges are linked into the audit budget. We need to recover whatever it costs to provide the audit service and the main annual cost components are shown in Table 6.1.

TABLE 6.1 Audit cost profile.

Item	£
Salaries	
Staff expenses	
Office accommodation	
General admin. overheads	
Equipment	
Other expenses	
Total cost	

By dividing the total annual costs over the projected number of chargeable audit hours for the year (normally 214), we can arrive at a recovery hourly rate. By increasing this hourly rate we may achieve a trading surplus as a contribution to non-recoverable time and purchases such as expenditure on computer equipment. The hourly charge-out rate will vary by grade of auditor and this factor will be entered into the time monitoring system. Alternatively, a rough indicator of the hourly rate may be calculated by using the following formula:

$$\text{Hourly rate} = \frac{\text{Annual salary } (\times 1.5)}{\text{Chargeable hours for the year}}$$

Service Level Agreements

Service level agreements (SLAs) may be defined for each department audited and involve the following:

1. Define the audit strategy based on the wider organizational strategy.
2. Carry out a general survey of business risk areas by reviewing the corporate risk database.
3. Discuss the results with management.
4. Agree to an annual plan as a result.
5. Take the draft annual plan to the audit committee.
6. Cost out the financial implications of the agreed audit services.
7. Produce a costed SLA for formal confirmation by the various directors.
8. Take the agreed and priced annual plan to the audit committee.

The time charging system will allow audit management to monitor the extent to which the budgeted income is being achieved and this will be reported quarterly to audit management. The audit committee, as well as having a general overseeing role, may also request certain reviews and will be charged accordingly. The CAE will probably advise the audit committee on any necessary corporate reviews. Note that management should not generally be able to refuse a planned audit review, but may negotiate the timing or ask to negotiate additional work where there are sufficient audit resources available. Managers may in addition request details of audit's planning, risk analysis and time charging mechanisms.

Creating the Audit Image

Audit needs to formulate and maintain an appropriate image and one auditor who breaches professional behaviour may tarnish the reputation of the whole department. The audit image is based around the standards set out in the audit manual and the auditor code of conduct. In addition it requires the following features of the internal auditor:

- politeness, having regard to the need to respect fellow officers at whatever grade;
- being positive by building constructive working relations with management;
- sensitivity to management's needs;
- respect for confidentiality with an understanding of the damage that idle gossip can do;
- a team-based audit approach working with and alongside management;
- a hard-working attitude with a constant mission to encourage management to promote good controls;
- a desire to explain the role of audit and promote the audit service wherever possible.

It may be an idea to organize a series of seminars (or a slot at the corporate annual conference) and deliver the new-look internal audit approach.

The Published Annual Report

The internal audit department will publish an annual report after the confidential annual activity report has been considered by the audit committee. This will cover the work carried out and services provided, and has the role of a general information document. It should be written in a public relations style to communicate the services audit may provide and how management may participate and incorporate its views into audit planning. Important concepts such as independence, behavioural aspects, audit approach, different perspective of external audit and so on may also be mentioned. This should be sent to senior management and be available on request, and via the internal audit website to all employees.

6.10 Continuous Improvement

To make a start on noting a few comments on the quality drive we can mention the points made by the founding father of the quality movement, Dr Edwards Deming:

1. An organization must have a consistent message about quality.
2. There must be a commitment to change and continual improvement.
3. Defect prevention rather than detection.
4. Build partnerships with suppliers.
5. Constantly improve.
6. Train in a way which makes everyone responsible for their own quality.
7. Supervision must encourage and support, not chase.
8. Drive out 'fear' of improvement.
9. Break down department barriers to foresee problems and improve quality.
10. Don't set unrealistic targets.
11. Enable employees to have pride in their work.

12. Train and educate.
13. Create an organizational structure which supports all of the above.

Returning to the internal audit dimension, Charlie Farrow has made his suggestions about the marketing angle:

> Pitfalls to avoid:
>
> - Don't mistake the outwardly visible evidence of marketing activity, in the form of advertising activity, brochures, editorial coverage, selling and the like, for marketing itself.
> - Don't believe that quality sells itself.
> - Don't believe that appearances don't matter.
> - Don't imagine there are any shortcuts.
> - Never boast.
>
> . . . Planning and preparation are essential for the successful implementation of any marketing activity.[18]
>
> Meanwhile, the three key drivers for the marketing campaign have been noted just as crucial to the survival of an in-house audit team:
>
> Many internal auditors have failed to appreciate what marketing can offer them and even worse, have become complacent about themselves and the role that they play within their organisation. Marketing can achieve many benefits not least:
>
> - the opportunity to truly demonstrate to the organisation the value added by internal audit.
> - the ability to raise internal audit's profile so that it is invited to the 'top table' and involved in key projects within the organisation.
> - the opportunity to ensure that the organisation does not consider outsourcing internal audit as a serious option.[19]

Selling the internal audit service has been tackled by George A. Ewert:

> If we internal auditors are to establish ourselves as management partners, we must market our function and its potential more effectively. New roles are earned, not handed out by companies. To encourage our employers to recognize how much they need us in every area of the business, internal auditors should concentrate on the six 'Ps':
>
> - *People – As the visible provider of audit services, internal audit staff are the backbone of a successful marketing strategy . . .*
> - *Process – Business processes can be separated into two categories: the processes used in managing and operating the audit business, and the process we can impart to operating management to help them understand and manage their business risk.*
> - *Perspectives – Through its objectivity and independence, internal auditing occupies a unique position in the organization . . .*
> - *Price – Another important aspect of a successful marketing strategy is attractive pricing. Customers generally have two concerns about price – that they obtain value for the money they spend . . .*
> - *Place – In internal auditing, place means anticipating and responding to the corporation's needs by examining areas with the potential to yield the most value, either in relation to risk or through the cost beneficial development of controls.*

- *Promotion – Promotion is the focus of many marketing strategies. It involves advertising – making people aware of the product and how it matches their needs – to increase and service demand. It also involves packaging that attracts the customer . . .*

In a successful marketing program, we demonstrate these beliefs, our capabilities, and our desire to be management's partner through consistent behavior with our staff and customers. This approach will reward us with innovative options for serving our organization.[20]

Finally, Drew J. Breakspear has given us six rules for successful internal auditing:

> We live in an age when every department is expected to add value. Internal auditing can no longer sit idly by and watch the business world from our ivory tower. We must realise that we are indeed a business, and that what works best in business will work best for internal auditing. Six essential rules of business:
>
> 1. Serve your customers. Learn from them. Be responsive to them and understand their business, technology, and operations. Find out what motivates them. Communicate with them. Make them your partner.
> 2. Make sure your products meet customer needs.
> 3. Constantly review your production processes. Think costs, and be sure the benefits outweigh the costs.
> 4. Know your competition, and be sure to maintain a competitive advantage. Think quality.
> 5. Improve. Constantly refresh your approach. Factor in changes in the environment and technology. Help your people grow and develop.
> 6. Market your skills, and sell them by doing and executing. Become an indispensable part of the team.[21]

It is important to keep the audit shop up to date and vibrant. Continuous learning is one way of avoiding stagnation and as we define new audit products, we need to ensure they are delivered in a way that promotes quality and value, meanwhile we should note that IIA Performance Standard 2040 requires that 'The CAE should establish policies and procedures to guide the internal audit activity.' The process in Figure 6.10 may be applied to turning ideals into procedures and into products.

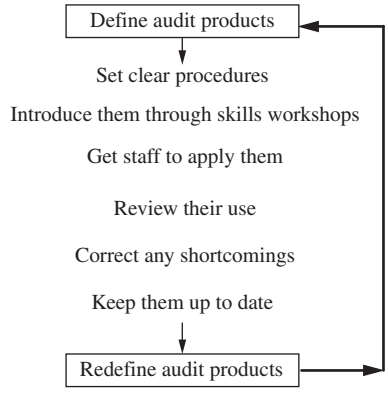


FIGURE 6.10 Procedures cycle.

Having worked out what our clients expect from internal audit, we can refine our procedures for service delivery. Regular staff workshops and skills update events are an important part of quality services. Working around new products, we can make sure they are understood and applied properly and look carefully at any shortcomings that impair the impact of our work, on both assurance and consulting fronts. A continuous revolving cycle of updating, improving and involving staff in cultivating their skills both new and improved should underpin the audit business and marketing strategy. Having the following three mechanisms in place promotes continuous learning and success:

1. a clear role definition and service base that responds to changing needs of stakeholders;
2. procedures that are efficient, flexible and focused on achieving service delivery standards;
3. a staff development system that ensures continuous revitalization of skills, attitudes and approaches.

This depends on audit management considering many wider issues concerning quality standards and how they are applied, which is a far cry from issuing the occasional obscure memo to staff on new procedures.

6.11 New Developments

A major dilemma that has continued to rage for some time now relates to ways that the efficiency of the internal audit function can be assessed. There is an abundance of different measures in use and some are better than others. Bearing in mind the importance of efficiency in the way audit resources are applied means effective measures are always welcome, including those suggested by PwC:

- Internal audit department costs compared to budget
- Number of audits completed in accordance with the scheduled audit plan.
- Number of integrated audits (operational and IT auditing).
- Internal audit department cost per internal audit full-time equivalent.
- Internal audit department cost components.
- Reduction in internal audit effort and/or increase in audit coverage due to use of data-mining and data-analytics technologies.
- Staff utilization (% of time charged to non-administrative audit tasks and amount of overtime).
- Cost savings generated by implementing audit recommendations.
- Average time it takes to issue an audit report.[22]

The IIA.UK&Ireland has developed a six-step CPD process that involves each auditor taking charge and self-assessing their personal position, which is as follows:

1. self-assessment to identify training and development needs and aspirations;
2. target-setting for development in terms of outcomes;
3. creation of a development plan;
4. engagement in suitable activity;
5. monitoring and review of development plan;
6. critical reflection.

Auditor competency is another key concern as we move from the financial/compliance perspective to one that considers all aspects of an enterprise wide risk management process. The IIA has built a competency framework that covers:

- interpersonal skills
- tools and techniques
- internal audit standards, theory, and methodology
- knowledge areas.

The idea is to develop the ideal auditor and since IT is a core area it is integrated throughout the framework. This ideal auditor is able to consider risks as negative threats and risks as positive opportunities that others will grasp if simply sidestepped. Auditor competency sits high on the CAE's agenda and this includes good interpersonal skills. Besides working with senior people, the internal audit is required to get along with internal assurance teams:

> Respondents expect to work much more closely with other assurance providers by 2012. Interaction is currently only "limited" with assurance functions related to the environment, CSR, insurance and health and safety. They do already consult and share information with management, compliance and external audit – by 2012 they expect to rely more on each other's work to avoid duplication. None of the respondents said they had a fully integrated assurance plan.[23]

Finally, we look at the way internal audit is resourced with the view that auditors are now talking to more senior people as they work on high risk projects and strategic parts of the business. Steve Bundred gives some advice on how to meet this challenge:

> The best-performing internal audit functions employ professional people – at least in the senior roles – and have "clout", says Bundred. They work in organisations where risk management processes are embedded, and will have contributed to achieving that. They will be influencing the way in which managers across the organisation think about the internal control environment when they're managing change processes, when they're introducing new systems, or when they're re-engineering business processes, he adds. "The question is: how strong is the culture of the risk control environment and what contribution has internal audit made to that?" Improving the quality of internal audit is not just a matter of telling internal audit functions to do better, says Bundred. Internal auditors need to look higher up the organisation, influencing the top people about where internal audit should be and persuading them of the contribution that good internal audit can make to the way the organisation is run.[24]

Summary and Conclusions

The quality movement has been established for many years and there are various standards, guidelines and tools that can be used to incorporate quality into the internal audit shop. Moreover, there are benchmarks, measures and full-blown accreditation schemes that can be used so as to avoid reinventing the wheel. In one sense, we could argue that an independent review activity must have its own house in order before it can embark on this review activity with any real credibility. The IIA standards make it clear that there must be a system of QA in place and that any non-compliance should be formally reported. There is also a need to secure 'audits' of the

auditors to ensure a sense of fair play. In an IIA member needs survey in 2001, 50% of more than 1,300 IIA members reported that they had never experienced an external QA review. All IIA audit shops will need to engage a formal external review at least once every five years and this somewhat simple requirement brings to bear a major process for isolating problems in internal auditing that may have sat quietly as nagging concerns for many years. External reviewers will ask: What is the system for assuring quality in use in this internal audit shop, is it adhered to and does it work in practice?

This very same question should sit at the top of the CAE's agenda. Real quality happens when the CAE, audit managers, senior auditors, team leaders and basic audit grades ask the parallel question: What is the system for assuring quality in use in this internal audit shop and have I developed myself so that I can live up to the set standards and ensure it works in practice?

When internal audit has arrived at this juncture, quality will be secured and it is only a matter of developing strategies for adjusting quality systems to meet the changing needs of stakeholders. One way of getting people involved in the quality equation is to set up a CRSA workshop where we consider the risks that confront the internal audit mission and go through the usual tasks of prioritizing and managing key risks, in the context of the adopted quality management system. We can repeat here the crucial demands set by Attribute Standard 1320 which states that 'The CAE must communicate the results of the quality assurance and improvement program to senior management and the board.' There is no room for complacency where any gaps in quality management will be placed in front of the top executives. Major gaps will question the ability of internal audit to deliver the audit objective and may undermine the whole basis of assurance, as well as consulting work. The final point to note regarding quality systems is the need to sell the audit mission. If this is proving difficult, then reference may be made to the IIA.UK&Ireland's website (www.iia.org.uk) where the real value from internal auditing is described:

> The need for organisations to manage a wide range of risks including regulatory, legal, reputational, market, liquidity and operational is becoming increasingly critical as organisations strive to achieve demanding goals and manage stakeholder expectations. In turn, the demands and expectations being placed on internal auditors are significantly increasing as executives and operational management look to the internal auditor for assurance and risk management and control-related advice. Over the next decade the role of the internal auditor will become one of the most demanding, yet rewarding, in corporate life.

There is really no excuse for failing to reach the exacting levels of performance and profiles that many internal audit shops are achieving. Professional standards abound, and the IIA with its professional practices framework have been knocking on the boardroom door for many years now. The last ten years have seen a major shift in the roll call of professional disciplines that has placed internal auditing right up there with the accountants, lawyers, top flight consultants, business analysts and so on. Professional standards create the targets that need to be aimed at, even where the audit shop is small. It is essential that each internal audit team tracks developments in the professional standards and incorporates new aspects into their own policies and interpretations of the audit role. In considering just what we are aiming at when developing and using audit standards, we can refer to the vision provided by Jean-Pierre Garitte, a past chairman of the IIA:

> Internal auditors are not effective in today's environment unless they have found ways to earn the respect and trust of their clients. Bridges cannot be built unless those on each side recognize the benefits of being connected and understand a common need. For these bridges to be functional and vital, they must be engineered around the business objectives of the organization. Internal auditors can not only be the architects – those who envision how it can happen – but

they can also be the engineers, those who spearhead a spirit of unity and collaboration. In our efforts to succeed, and if we are to win trust, the competence and objectivity of internal auditors must be given. There can be no confusion about 'whose side the auditor is on,' and no uncertainty about whether or not we can produce what is needed. The auditor has a job to do; but that job must be accompanied within the context of a deep and clear understanding of why we exist: to help the organization and its people. Our function and activities must be based on a strong sense of organizational mission: on how we can best perform our role as management agents; and on both a systematic and common-sense approach to risk management.[25]

Chapter 6: Assignment Questions

Having worked through the chapter the following questions may be attempted (see Appendix A). Note that the question number relates to the section of the chapter that contains the relevant material.

1. Explain why professional internal auditing standards are important in enhancing the role and status of the internal auditor.
2. Describe the framework of the IIA standards and list some of the areas covered in a selection of the Attribute and Performance Standards that are issued by the IIA.
3. Discuss the need for exercising due professional care when performing internal audits and explain why this is becoming increasingly important.
4. Describe the different types of consulting services that may be performed by the internal auditor and explain how management consultants also work to professional standards.
5. Explain why quality is important to the internal audit service, and describe steps that may be taken to ensure quality standards are defined, enhanced and applied by internal audit staff.
6. Discuss why it is important for internal auditors to have a clear view of the various clients for their services.
7. Contrast internal and external reviews of the internal audit shop and describe the areas that may be addressed by an external review of internal audit.
8. Describe the use of one of the following four management techniques: ISO 9000, Charter Mark, EFQM, IiP.
9. Discuss why it is necessary to market the internal audit role and describe efforts that may be taken to ensure the marketing strategy helps secure the future prospects of the internal audit shop.
10. Prepare a presentation to the internal audit management team on how a successful internal audit service may be promoted through continuous improvement.

Chapter 6: Multi-choice Questions

6.1 Which statement is least appropriate?
There are ways that we can move closer to developing good auditing standards:
   a. We must recognize the practicalities of real-life auditing and formulate standards that provide statements of intent rather than comprehensive procedures.
   b. Encourage each organization to translate the standards into suitable work practices and incorporate them into the audit manual.
   c. Make compliance with the spirit of the standards a major issue that is uppermost in the minds of all staff. To this end any barriers to compliance should be addressed.
   d. Ensure that staff who are not trained to meet all the requirements of the standards are transferred out of internal audit.

6.2 Insert the missing words:
Standards play a crucial role in internal auditing and support the concept of auditing as a professionally based discipline. It is however clear that published statements are of little use unless they have been fully implemented and subject to continual review. The ..... is the right mechanism for this process and it is through this that formal standards may be set and adopted.
a. bonus scheme
b. audit manual
c. performance appraisal scheme
d. working paper file

6.3 Insert the missing words:
A ..... attaches to the discipline and is to be mastered. This represents a minimum level of knowledge that is studied and understood.
a. level of understanding
b. common understanding
c. basic level of knowledge
d. common body of knowledge

6.4 Which item is least appropriate?
There are various hallmarks of professionalism:
a. Training programme
b. Common body of knowledge
c. Code of ethics
d. Sanctions
e. Reports to regulators
f. Control over services
g. Qualified practitioners
h. Morality
i. Technical difficulty
j. Examinations
k. Journals
l. Professional body
m. Compliance with rules
n. Service to society

6.5 Which item is wrong?
The IIA has described its original objectives in 1941 when it was first established:
a. to cultivate, promote, and disseminate knowledge and information concerning internal auditing and subjects related thereto;
b. to develop, promote, and disseminate knowledge and information concerning internal accounting procedures;
c. to establish and maintain high standards of integrity, honour and character among internal auditors;
d. to furnish information regarding internal auditing and the practice and methods thereof to its members.

6.6 Indicate whether the listed services are assurance or consulting services:
The definition of internal auditing makes it clear that it is an assurance and consulting activity including the following types of engagements:

	Assurance	Consulting
a. advice		
b. compliance		
c. counsel		
d. due diligence		
e. facilitation		
f. financial		
g. process design		
h. systems security		
i. training		

6.7 Which statement is most appropriate?

a. The primary players in assurance work are the auditor and the party to whom assurance is being provided, while for consulting work it is simply the auditor and the client.
b. The primary players in assurance work are the auditor, the client and the third party to whom assurance is being provided, while for consulting work it is simply the auditor and the client.
c. The primary players in assurance work are the auditor, the client and the audit committee to whom assurance is being provided, while for consulting work it is simply the auditor and the client.
d. The primary players in assurance work are the auditor, the client and the third party to whom assurance is being provided, while for consulting work it is simply the auditor, the client and the audit committee.

6.8 Which statement is least appropriate?

Some of the barriers to good quality include:

a. A failure by audit management to recognize (and/or understand) the importance of quality assurance systems.
b. An emphasis on securing relevant audit evidence to support audit reports.
c. Poor management information systems that fail to provide feedback on performance targets.
d. A redundant audit manual that is not able to act as the vehicle for defining and using audit procedures.
e. Internal audit departments that have failed to adopt good change management techniques which means that new procedures become very difficult to install.
f. An absence of formal audit strategy leading to a lack of direction.
g. An absence of human resource management practices, such as formal training programmes, leaving staff to "sink or swim".
h. A failure to appreciate the need for client-based systems that enable service recipients to specify their needs and expectations in respect of internal audit services.

6.9 Which statement is least appropriate?

We would look to our systems to tell us whether internal audit is meeting the requirements of these standards. This entails the following:

a. Adopt suitable professional standards (e.g. IIA) as part of the formal mission statement that drives and directs the audit service.
b. Redefine the above as local standards via suitable enclosures in the audit manual.

c. This creates an assimilation of outline standards into working practices as a necessary step towards fully integrating them into the audit role.
d. Implement them via a formal procedure whereby staff are advised as to the requirements of these standards and so understand all that this entails.
e. Train and develop staff to meet them.
f. Review compliance with standards via suitable control mechanisms.
g. Deal with any non-compliance without making this a serious issue.
h. Review these standards to ensure that they make sense and fit with the audit work that is performed.
i. Seek to relate quality problems with these standards in terms of gaps therein or non-compliance.

This is in full recognition of the systems approach to problem solving where all operational defects are related to deficiencies in the underlying systems.

6.10 Insert the missing word:

. . . . . is fundamental to audit management that seeks to isolate potential problems before they arise. This requires ongoing involvement of senior auditors in their staff's work, providing advice and guidance.

a. Supervision
b. Professionalism
c. Standardization
d. Precision

6.11 Which statement is least appropriate?

The reviewer must ask questions such as:

a. What were the procedures relevant to this audit?
b. Have these procedures been fully communicated to the auditor who carried out the work?
c. Is there sufficient evidence of compliance with these procedures?
d. Is there any evidence of non-compliance with these procedures?
e. Does the audit mission need to be re-stated?
f. Is there any explanation for apparent non-compliance?
g. Has the audit been a success?

6.12 Which statement is least appropriate?

Best practice concerning the use of procedures that have been breached should make them comply with several criteria before they may be used in disciplinary action against an employee:

a. Procedures must be clear and concise.
b. They must be fully communicated to staff.
c. Their status should be set out, whether they constitute instructions, rules, advice or explanations.
d. The people who are affected should be clearly identified along with any measures to deal with further information or guidance that may be required.
e. They should explain how compliance will be monitored and what are the staff's responsibilities in assisting this process.
f. The role of any warnings that will be given for instances of non-compliance.
g. The consequences of non-compliance must be defined, particularly where this is serious, e.g. a disciplinary and possible summary dismissal.
h. Important procedures should be reissued regularly and meetings used to convey their importance.

i. They may form part of the induction training for new starters.
j. Any non-compliance, even if it was not deliberate, may be used for charges of gross misconduct.
k. They should be fair, consistently applied and meaningful.

6.13 Which statement is most appropriate?

a. Professionalism and quality is about giving the client what they both want and need. This simple concept becomes more involved for internal auditors because we have several different stakeholders and because we deliver both assurance and consulting services. Nowadays, people who receive audit services are simply known as auditees.
b. Professionalism and quality is about giving the client what they both want and need. This simple concept becomes more involved for internal auditors because we have several different stakeholders and because we cannot deliver both assurance and consulting services. In the past, people who received audit services were simply known as auditees.
c. Professionalism and quality is about giving the client what they both want and need. This simple concept becomes more involved for internal auditors because we have several different stakeholders and because we deliver both assurance and consulting services. In the past, people who received audit services were simply known as clients.
d. Professionalism and quality is about giving the client what they both want and need. This simple concept becomes more involved for internal auditors because we have several different stakeholders and because we deliver both assurance and consulting services. In the past, people who received audit services were simply known as auditees.

6.14 Which statement is least appropriate?

a. Internal reviews involve an extensive review of overall audit strategy, staffing levels and budgets.
b. Internal reviews may operate at a number of levels including reviewing the working papers and draft audit reports.
c. One should develop a programme of audit reviews where audit management will carry out comprehensive reviews of say the bigger audits that have been completed.
d. Spot checks may be undertaken at random on various audits to establish whether they are meeting acceptable standards.
e. It is advisable to appoint one manager responsible for quality assurance throughout the audit department.
f. This person will report periodically, (say annually) to the CAE on the overall position

6.15 Relate the concepts 1–4 to the descriptions a–d

There are various marketing concepts:

1. The production concept
2. The product concept
3. The selling concept
4. The marketing approach

There are four different descriptions that relate to the above concepts:

a. will concentrate on the audit itself and suggests that so long as the work is good and the report is done to quality standards everything will be fine.
b. seeks to minimize the costs of the audit, which translates to the number of hours spent on each individual project.
c. takes the view that we must first find out what is required by the organization and then seek to meet these requirements.
d. we need only ensure that the client pays for our services, which may be mandatory in most organizations who resource an audit function.

Concepts	Descriptions a, b, c or d
1	
2	
3	
4	

6.16 Which statement is most appropriate?
A formal complaints procedure should be applied whereby management is advised of a clear process for submitting their concerns. The introductory memoranda to management may include the following paragraph:

a. We hope that you will not experience any problems with the audit work since all auditors work to the highest professional standards. However should you have any particular concerns please voice them to X who is the team leader for this project. In the event that you are still not satisfied please ask the team leader to contact the CAE.
b. We hope that you will not experience any problems with the audit work since all auditors work to the highest professional standards. However should you have any particular concerns please voice them to X who is the team leader for this project. In the event that you are still not satisfied please contact the CAE.
c. We pray that you will not experience any problems with the audit work since all auditors work to the highest professional standards. However should you have any particular concerns please voice them to X who is the team leader for this project. In the event that you are still not satisfied please contact the CAE.
d. We hope that you will not experience any problems with the audit work since all auditors work really hard. However should you have any particular concerns please voice them to X who is the team leader for this project. In the event that you are still not satisfied please contact the CAE.

6.17 Insert the missing words:
It is important to keep the audit shop up to date and vibrant. ..... is one way of avoiding stagnation and as we define new audit products, we need to ensure they are delivered in a way that promotes quality and value.

a. Continuous learning
b. Constant updating
c. Professionalism
d. Asking questions

6.18 Which statement is least appropriate?
Having the following mechanisms in place promotes continuous learning and success:

a. clear role definition and service base that responds to changing needs of stakeholders.
b. procedures that are efficient, flexible and focused on achieving service delivery standards.
c. a staff development system that ensures continuous revitalization of skills, attitudes and approaches.
d. detailed audit manual that covers every eventuality.

References

1. ACCA, 'Ethics and the accountant in the public sector', Mar. 1999, p. 8.
2. Wynne Andy 'Spotlight on internal audit'. *Public Finance*, 17–23 Sept. 1999, p. 28.
3. Control Captain 'Is there really a future for internal auditing?' *Internal Auditing*, Jan. 2000, p. 20.

4. IIA Research Foundation, founded in 1976 by the IIA, Objectives.
5. Kubr Milan (ed.) (2002) *Management Consulting, A Guide to the Profession*, 4th edition: International Labour Organisation, p. 10.
6. Kubr Milan (ed.) (2002) *Management Consulting, A Guide to the Profession*, 4th edition: International Labour Organisation, p. 5.
7. Sawyer Lawrence B. and Dittenhofer Mortimer A. (1996) *Sawyer's Internal Auditing*, Assisted by Scheiner James H., 4th edition, Florida: The Institute of Internal Auditors, p. 1264.
8. Sawyer Lawrence B. and Dittenhofer Mortimer A. (1996) *Sawyer's Internal Auditing*, Assisted by Scheiner James H., 4th edition, Florida: The Institute of Internal Auditors.
9. Figg Jonathan 'Power staffing 101'. *Internal Auditor*, April 1999, p. 22.
10. 'Abbey Road'. *Internal Auditing and Business Risk*, Aug. 2002, p. 29.
11. Chambers Andrew (2002) *Corporate Governance Handbook*: Tolley's, Reed Elsevier (UK) Ltd, p. 22.
12. Howard Clifford J. Jr. 'Narrow band'. *Internal Auditor*, April 1998, pp. 65–68.
13. Glascock Kenneth L. 'Auditees or clients'. *Internal Auditing*, Aug. 2002, p. 84.
14. *Internal Auditing and Business Risk*, Feb. 2001, pp. 28–29.
15. Reding Kurt F., Barber Craig H. and Digirolamo Kristine K. 'Benchmarking against CFIA'. *Internal Auditor*, Aug. 2000, pp. 41–46.
16. (2002) *Internal Auditing, Distance Learning Module*: Institute of Internal Auditors, UK&Ireland.
17. Leithhead Barry S. 'Ensuring audit relevance'. *Internal Auditor*, April 2000, pp. 68–69.
18. Farrow Charlie 'Marketing internal audit'. *Internal Auditing and Business Risk*, Sept. 1998, p. 20.
19. 'Lex service: marketing internal audit effectively'. *Internal Auditing and Business Risk*, Nov. 2000, p. 30.
20. Ewert George A. 'How to sell internal auditing'. *Internal Auditor*, Oct. 1997, p. 54.
21. Breakspear Drew J. 'Run it like a business'. *Internal Auditor*, Feb. 1998, p. 29.
22. Business upheaval: Internal audit weighs its role amid the recession and evolving enterprise risks, State of the internal audit profession study, PricewaterhouseCoopers 2009, PricewaterhouseCoopers' fifth annual state of the internal audit profession study, p. 23.
23. Towards a blueprint for the internal audit profession, Research by the Institute of Internal Auditors, – UK and Ireland in association with Deloitte, Deloitte & Touche and the Institute of Internal Auditors – UK and Ireland, 2008, p. 11.
24. Internal Auditing & Business Risk, IIA Magazine, Audit centre stage, Internal Auditing. May 2008, Steve Bundred, tells Neil Baker, pages 18–21
25. Garitte Jean-Pierre, Chairman of the IIA.Inc., *Internal Auditor*, Aug. 1998, p. 28.

Chapter 7

THE AUDIT APPROACH

Introduction

Internal auditing may be performed in many different ways and there are a variety of models that may be applied to discharging the audit role. The organization will define its audit needs and this will help to establish the types of audit services that are provided. The CAE is then charged with providing this service to professional auditing standards. This chapter explores some of these different approaches and the way that they relate to the role of internal auditing. The development of internal auditing, as a profession, is based on the premise that the practice of internal audit is a defined discipline subject to professional standards. At the same time, it is clear that there is a great deal of variety in the way the audit role is discharged. This results from different approaches and, in some cases, a different interpretation of the underlying principles, although the wide variety of audit-based terms does not necessarily mean that there is no clear discipline of internal auditing. It is not merely common-sense work that any untrained person may perform. What is evident is the way that the audit role is discharged will vary according to the agreed terms of reference (or audit charter). Variety creates a richness and degree of flexibility in the type of audit work that is undertaken. In many cases an audit department will contain different types of auditors who collectively discharge the audit function. Internal auditing is about evaluating risk management and internal controls and this should be a central theme in most audit work.

Systems Auditing

This is seen by some as the principal way in which the audit role should be discharged as it necessarily involves evaluating systems of internal control. The idea is that systems are studied to assess whether they are sufficiently controlled so that managerial objectives may be achieved. Before an opinion can be determined, it is necessary to test the operation of controls and the extent to which weaknesses impact on the end product. These tests may well include vouching, verification and an assortment of checks and confirmatory routines, the point being that vouching here is used as a technique to assist the control evaluation, as opposed to the results being an end in themselves. In this way, the emphasis is not on performing an endless series of tests but more on reviewing the system and its principal objectives. We start with the standard approach in the guise of systems-based auditing (SBA). The new context is to direct audit resources at the systems of corporate governance, risk management and controls. Control risk self-assessment (CRSA) has been used by many internal auditors as a way of getting work teams to identify and manage their key risks and the material on CRSA is complemented by a brief account of facilitation skills, as a prerequisite to performing the CRSA workshops. We also cover fraud and other investigations, IS (information systems) auditing and a consulting approach to work in recognition of the new directions that internal auditors are taking. Technology moves very quickly and Dan Swanson has provided some useful contributions to the Internal Auditing Handbook with a view to updating its coverage of IS auditing.

Note that all references to IIA definitions, code of ethics, IIA attribute and performance standards, practice advisories and practice guides relate to the International Professional Practices Framework (IPPF) prepared by the Institute of Internal Auditors in 2009. The sections addressed here are as follows:

7.1 The Systems Approach
7.2 Control Risk and Self-assessment
7.3 Facilitation Skills
7.4 Integrated Self-assessment and Audit
7.5 Fraud Investigations
7.6 Information Systems Auditing
7.7 Compliance
7.8 Value for money (VFM), Social and Financial Audits
7.9 The Consulting Approach
7.10 The 'Right' Structure
7.11 New Developments
Summary and Conclusions
Assignments and Multi-choice Questions

7.1 The Systems Approach

There are many different ways that internal auditing may be approached and some are investigatory/transactions-based while others move towards a systems approach. There is an argument that the most efficient use of audit resources occurs where one concentrates on reviewing systems as opposed to the examination of individual systems' transactions. Management may wish to use internal audit for one-off problem-solving exercises particularly where there is a potential embarrassment factor if the matter is left unresolved. On the other hand, where systems reviews are not carried out, then breakdown and suboptimal functioning may occur. This leads to delinquent transactions. It is possible to use force-field analysis to weigh up the factors that together define the actual audit approach that is applied in any organization. These forces have been set out in Figure 7.1:



FIGURE 7.1 Factors impacting on the audit approach.

Each of these factors will apply pressure in defining the way that the audit role is discharged and some of the influences may appear as shown in Table 7.1.

TABLE 7.1 Factors: main requirements.

Body	*Requirements*
The CAE	Review of systems of risk management and satisfying audit committee, the board and other audit clients
Audit committee	Systems of corporate governance, risk management and control validated, and accounting and accountability issues resolved
Line management	Management problems solved and help with establishing good risk management
Professional practice	Assurance and consulting role of internal audit

Performance standards 2100 – Nature of work

In terms of professional standards, there are aspects of an organization that clearly fall within the scope of audit work. Performance Standard 2100 means that the internal audit activity must evaluate and contribute to the improvement of governance, risk management and control processes using a systematic and disciplined approach. In terms of systems work, Performance Standard 2110 asks that the internal audit activity evaluates and contributes to the improvement of governance, risk management and control processes using a systematic and disciplined approach, while Performance Standard 2120.A1 makes it clear that the internal audit activity must evaluate risk exposures relating to the organization's governance, operations and information systems regarding the:

- reliability and integrity of financial and operational information;
- effectiveness and efficiency of operations;
- safeguarding of assets;
- compliance with laws, regulations, and contracts.

These systems need to be assessed by internal audit as part of the assurance role. There is a choice in the way internal auditing is carried out and although professional standards do set conceptual guidelines, they do not promote a particular methodology. The final approach will result from a combination of factors that affect the audit role and resultant work carried out. The premise upon which the Handbook is founded considers risk-based systems auditing as a valid interpretation of the assurance role of internal audit, with all other matters falling under the generic term investigations – most of which is part of the consulting service along with direct assistance and advice in establishing business risk management. The systems approach to internal auditing has provided an extremely powerful technique for conducting audit reviews and in the past has led to a change in auditing concepts. This requires an audit policy that stresses the importance of establishing good systems so that risks such as failure, errors and abuse may be avoided in the first place. Management is charged with devising and maintaining these systems with advice from internal audit. The move is away from error spotting, with more emphasis on getting the system of risk management right. Systems auditing is based on systems theory and wider systems concepts.

Features of Systems

Systems thinking is based on viewing operations and events as processes with the flows as shown in Figure 7.2.

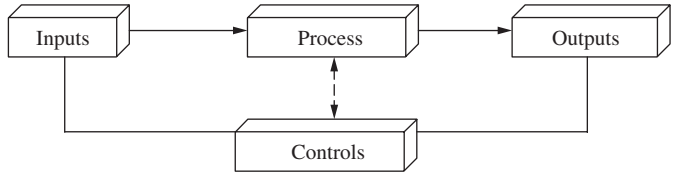


FIGURE 7.2 A basic system.

Defining a system:

> A set of objects together with relationships between these objects and their attributes connected or related to each other in such a manner as to form an entirety or whole.

There are a number of concepts that underpin systems theory and these may be listed:

Connected components Each part of the system has some relationship to the other parts, so that together they comprise the system at hand. For example, a link in a chain is connected by the two links that attach it to the chain as well as being connected to the other links by their relative position in the chain. Each link has a different proximity to the others but they still have some kind of overall relationship.

Affected by being in a system The components must be affected by being in the system in that there is some reason for it to be defined in this way. Going back to the chain, the links must be part of the process of forming a whole with the other links for the system to exist. A spare link that is not attached is not affected by the activities of the chain and so falls outside the system.

Assembly of components does something This brings into play the important concept of systems objectives which means that the system must have some purpose that justifies its existence. A bicycle chain drives the wheels while a gold chain worn around the neck will exist mainly for ornamentation.

Assembly identified as being of special interest This is the most difficult part of the systems concepts in that there must be an underlying reason why something has been defined as a system. A system depends on what is being defined rather than being an absolute concept. If we view a bicycle chain as a system consisting of links, this may be because we wish to examine its properties so that its strength may be improved. We can alternatively define the system as comprising the chain and the pedals if we wish to consider the way energy is transferred from the pedals to the wheels via the chain. This may be to seek to improve the efficiency of this energy transfer. The system is deemed to be a system because we wish it to be so, which brings in the idea of it having a special interest. Something becomes a system because people see it as a system. This point has been made clear by experts in systems thinking: 'We shall see that very often the most critical point for leverage in any system is the belief of the people in it, because it is the beliefs that sustain the system as it is.'[1]

The universal principles behind systems thinking can be applied in a wide variety of situations and there are several key features:

- An open system is linked to the environment and should respond to changes in relevant external factors so as to optimize the systems process. A closed system by contrast is fixed and does not react to external pressures. So a central heating system may remain on for fixed time periods controlled by a timer and once set remains in this mode of operation. Where there are thermostat controls, the system is able to respond to changes in the temperature and so provide a more interactive service. Controls are part of this process of adjusting the system to ensure it is always able to deliver its defined objectives.
- A system is a set of interrelated components and the idea of synergy comes into play. This suggests that the sum of the whole is greater than the sum of each individual component, which is expressed as:

$$2 + 2 = 5$$

- Synergy may be seen in the example of a series of parts that go to make a motorcycle. When stripped down, each part is a non-functioning component. When put together to form a motorcycle, it becomes a transportation system with far greater potential in terms of ability and horizons.
- Systems thinking is based on the idea of seeing a process as a whole, made up of related parts. This holistic view enables one to understand complicated operations by rising above each specific aspect and considering the whole. A major advantage of systems thinking is this potential for working at the highest levels by viewing an operation as a complete service. The auditor who is able to distinguish between low-level detail and material issues is the auditor of tomorrow. Viewing a system as a subsystem that feeds into a 'big picture' is a skill that the auditor should acquire.
- Key components are important parts that are crucial to the success of the process. Attention directed towards these will be of more value than the less material parts. The ability to isolate the key issues facing a managerial system has a fundamental impact on internal audit as our work moves towards higher levels in the organization. For example, there are many control weaknesses that are derived from problems with the human resource management systems. As the auditor progresses in the work, this factor may allow resources to be directed at this area as the most efficient use of audit time. The way the HRM systems interface with line operations can be captured by applying the systems view of the organization as both strong and weak links are isolated.
- Another theory derived from systems theory is that there are compensating influences. These can make up for weaknesses elsewhere in the system or simply provide an additional control. For example, a corporate financial system that is supposed to underpin budgetary control may be poor and only report actual spend after a delay of several months. Management may maintain its own record of spending to get up-to-date information of budget variances. The budgetary control system must be seen to include this compensating control if it is to be fully appreciated.
- In addition to the key components, there are sensitive areas in any system. The dependency chain means that the whole process may be at risk where parts of the link are weak or break down. It is only by understanding the whole system that one is able to determine the effect of changes in any one area on other linked areas. This may be the single biggest benefit to accrue from adopting a systems approach in contrast to viewing individual operations and activities as discrete items. The importance of controls in systems has been recognized by many as an example illustrates:

> David Blunkett faced fresh demands for urgent action to end the 'scandal' of illegal immigrants posing as students to get visas to stay in Britain. The Tories called for a crackdown after the

> *Evening Standard* found that unscrupulous language schools were taking cash payments to put 'students' on their books who were actually here to work illegally . . . A *Standard* investigation showed how four out of five schools approached in London were ready to issue a Czech journalist posing as a 'student' with a certificate of enrolment – virtually a sure-fire route to a visa – even when told explicitly that she would not be attending courses. The *Standard's* investigation raises concerns about our chaotic immigration system . . . We need some sort of control systems to stop private colleges fiddling the system.[2]

- All systems need to be in control to work and the ability to be in control is implicit in the feedback mechanism: 'Balancing feedback seeks a goal. All systems have balancing feedback loops to stay stable, so all systems have a goal – even if it is only to remain as they are . . . A system therefore needs a way of measuring, otherwise it could not tell the difference between where it is and where it should be.'[3]
- We turn to the issue of linkages and parent/child systems which interface with the activities that we are considering. Returning to our example of a motorcycle, the associated systems have been illustrated in Figure 7.3.

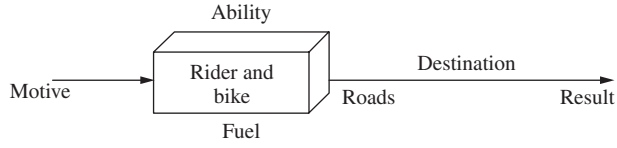


FIGURE 7.3 Motor cycle transport system.

The rider and bike may be seen as the primary system that then feeds into link systems such as roads, fuel and objectives. There is an infinite number of systems combinations that may be applied depending on one's perceptions. An audit terms of reference must state clearly where the system under review stops and starts. We need to establish the conceptual cut-off point as the motorcycle example can be extended to include maintenance, manufacture, cleaning, road maps, driving licence and VFM.

General Systems Thinking

A brief mention of systems theory and an overview of this methodology appear in Figure 7.4. Some explanations are provided below:

1. **Systematic.** The process of using a clear methodology is applied in SBA by using a defined methodology for planning, progressing the audit, and then issuing the audit report.
2. **Systemic.** This use of systems theory is applied to the way the audit field is viewed as a series of systems and link systems.
3. **Subjective system.** Here the use of a set system's boundary to define the system under review is something that auditors should apply to provide an agreed picture of what will be subject to audit.
4. **Parent system, main system and subsystem.** The appreciation of systems relationships in a hierarchical manner and as part of the associated system gives an insight into the way activities feed into each other.

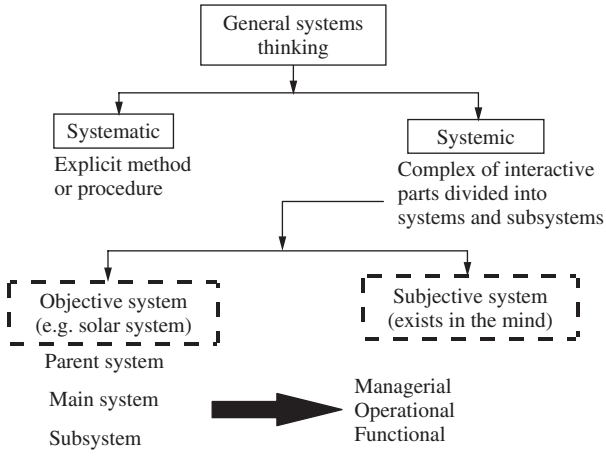


FIGURE 7.4 General systems thinking.

5. **Managerial, operational and functional.** The translation of systems to organizational levels and types gives a start to deciding how to break down the organization for audit purposes.

Entropy

This may be seen as a disorder, disorganization, lack of patterning or randomness of organization of systems. A closed system tends to increase in entropy over time in that it will move towards greater disorder and randomness. Entropy provides a justification for the audit role as systems break down and controls deteriorate over time unless they are reviewed and made to keep pace with changing risks. The trend to removing a tier of management to achieve budget reductions may have a major impact on systems controlled through supervisory reviews by line and middle management. The balance of controls should change with restructuring. If not, the imbalance becomes part of the overall entropy where a deterioration in controls impairs the successful functioning of the system. Systems are designed to ensure an objective is achieved in the best way possible and it has been said that 'Systems thinking is the way we can discern some rules, some sense of pattern and events, so we can prepare for the future and gain some influence over it.'[4]

Systems Auditing

We can use the principles of systems thinking to conduct systems audits. We are primarily concerned about the arrangements for effecting the four key risk exposures that fall within the scope of internal auditing Performance Standard 2110.A1:

- Reliability and integrity of financial and operational information
- Effectiveness and efficiency of operations
- Safeguarding of assets
- Compliance with laws, regulations and contracts.

We are concerned with reviewing and then advising management on their systems of internal controls that discharge these four objectives. So an activity should be undertaken with due regard for compliance with laws and procedures and this feature should be built into the system. Systems in control will subscribe to these key control features, in contrast to those that are at risk. There is one problem inherent in Performance Standard 2060 which includes the following line:

> The chief audit executive must report periodically to senior management and the board on the internal audit activity's purpose, authority, responsibility, and performance relative to its plan. Reporting must also include significant risk exposures and control issues, including fraud risks, governance issues, and other matters needed or requested by senior management and the board.

The problem comes from trying to take a view on risk management across the organization when we only have the results of individual audits at hand. Joseph O'Connor and Ian McDermott warn against the silo approach to viewing systems: 'Systems have emergent properties that are not found in their parts. You cannot predict the properties of a complete system by taking it to pieces and analysing its parts.'[5]

The Transactions Approach

Systems are designed to process transactions and internal audit is concerned with controls that ensure the system's objectives are met. Where this does not happen, the system produces delinquent transactions that breach one or more of the four key control areas. An audit approach that ignores the systems but seeks to identify delinquent transactions may be seen as a transactions-based audit. Probity visits, fraud investigations, compliance testing programmes, spot checks and VFM efficiency reviews may be based on the transactions approach. Any audit work that does not include assessing risks and evaluating and testing controls cannot be systems auditing. Systems auditing relies on some testing although this naturally flows from the review of controls shown in Figure 7.5.

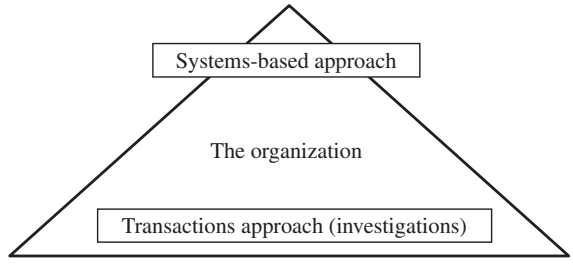


FIGURE 7.5 Systems versus transactions approach.

For example, an audit team may be used to follow company vehicles to see whether they were being used on official business. This displays adherence to a transactions-based approach, since a systems approach would seek to consider the controls that should be in place to ensure that vehicles are used only for business purposes. We might wish to observe several vehicles during

the course of the audit but this would be to check the way these controls are operating and not as an audit in its own right. A systems audit of a payments system will seek to isolate and review controls over the process of preparing invoices and paying suppliers. A transactions approach examines a sample of payments to see if they are correct and proper without commenting on the underlying controls. The main principle is that systems auditing starts from the top (controls established by management), in contrast to the transactions approach which starts at the bottom (the end results of transactions processing).

Stages of Risk-based Systems Auditing (RBSA)

Systems thinking is used twice in risk-based systems auditing (RBSA). First, we break down operations as systems, components of a system, subsystems, parallel systems and parent systems. An overview may be adopted and links between operations may be identified and understood. Second, RBSA is in fact a systematic audit approach in itself, with defined stages and clear links between successive steps. The stages of an SBA audit are shown in Figure 7.6.

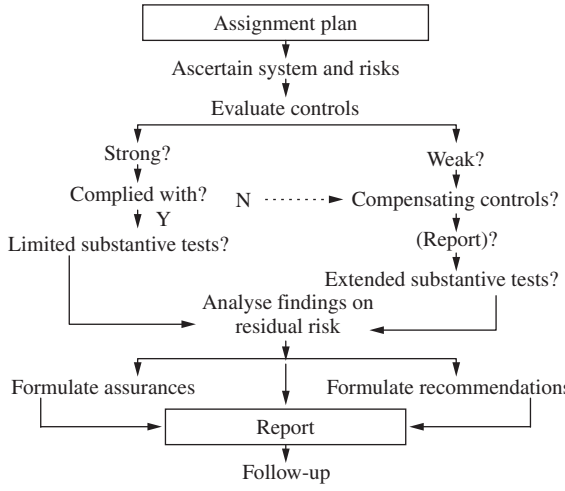


FIGURE 7.6 Risk-based systems auditing process.

RBSA cannot be carried out without following the above steps. Once the assignment plan has been determined (after a preliminary survey) we have clear terms of reference and an outline of the system in question. The next stage is to determine what risks may prevent the business goals from being achieved and ensure these risks are understood, classified and prioritized. Having discovered the key risks, we can go on to weighing up and evaluating the specific controls that form the main aspect of the risk management strategy and assess whether the controls are adequate. Adequate controls (strong) should be further considered to judge whether they are working properly through compliance tests. Some auditors argue that even when controls are in place and working, there needs to be a small amount of further testing to ensure the correct results are obtained (i.e. the system objectives are being achieved). Weak controls mean there is an unacceptable level of residual risk and this may be reported straight away. Again, some auditors wish to test the implications of these weaknesses and seek out actual error, abuse, failure

and other such risk exposures to demonstrate the implications of poor controls. The findings on the state of the residual risk lead into assurances where all is well and recommendations where there are further improvements needed to mitigate aspects of the residual risk that need to be contained. The results are reported back to the client and any action required monitored during a follow-up audit that is scheduled for the future. However, there is one word of warning. When an auditor tries to 'fix' a poor system it is much better to get the client to help in this process. This is due to the dynamic complexity in systems where they have internal forces that tend to pull things together. If these forces are not understood, then proposed changes will not work. These forces have been described as follows:

> A system will act like a strong elastic net – when you pull one piece out of position it will stay there for as long as you actually exert force on it. When you let go, you may be surprised and annoyed that it springs back to where it was before. Yet when you see this obstinacy as part of a system rather than isolated maliciousness, its resistance it not only understandable but inevitable.[6]

Returning to the stages of the RBSA, there are a number of matters to be considered at each stage:

Define clear objectives for the stage What we are aiming to achieve should be clearly stated at each stage so that the actual output can be measured against this.

Plan the work and approach to be adopted Planning is a continuous process that occurs before the audit and throughout the various above-mentioned stages. It is possible to set a separate time budget for the stage and then seek to monitor hours charged before finalizing the audit. It is also possible to carry out a review of work as the stage is completed to provide an ongoing supervision of the project by audit management.

Obtain a good understanding of the risks to the operation This may be achieved through analysis, discussion with client staff or through a structured workshop where the client team members consider their risks and how they impact on their business and team goals.

Define any testing strategy Testing is applied at ascertainment (walkthrough), compliance (after evaluation) and substantive testing (after evaluation and compliance tests). The detailed work programme may be drafted and agreed upon as the appropriate stage is arrived at.

Define the techniques that will be used Audit techniques such as interviewing, flowcharting, database interrogation, control self-assessment, negotiating and statistical sampling should be agreed again at the relevant stage of the audit. This will assist timing the work and enable additional upon skill needs to be identified.

Brief staff working on the project With a team approach, it is useful to break down each stage so that a briefing can be held to discuss problem areas, progress and other matters. Not only will this act as a feedback device but it will also promote team working where ideas are exchanged.

Ensure that the work is formally documented Standardized documentation ensures all key points are covered and that the work is fully recorded. The end of this stage is a convenient time to consider whether the documentation meets quality standards (according to the audit manual)

and contains all the necessary detail. The opportunity to obtain missing material is more readily available during and not after the audit. There is an obvious link between this and the audit manager review procedure.

Look for high levels of unmitigated risk It is good practice to report as the audit progresses to save time and ensure that the report is fresh and dynamic. The auditor has the opportunity to assess the impact on the work done so far on the report and the testing strategy that will have to be developed at some stage. Details of excessive risk can enter the report so long as the repercussions have been tested. Since evaluation of risk occurs throughout the audit, the whole package of views on the ability of key controls to mitigate risk is developed as work progresses. This is a major part of the auditor's work.

Agree on the direction of work for the next stage The link between stages comes naturally from the systems approach to auditing as one moves smoothly from one to another. The direction of the next stage must be considered by the auditor not only from a planning point of view, but also from the wider perspective of whether work should be expanded, curtailed or adjusted. This is the point at which to discuss matters with the audit manager and also advise that the stage in question is complete.

Key Systems Issues

In a RBSA, the auditor will comment on specific determinations of the state of controls that have been reviewed, as Figure 7.7 demonstrates.

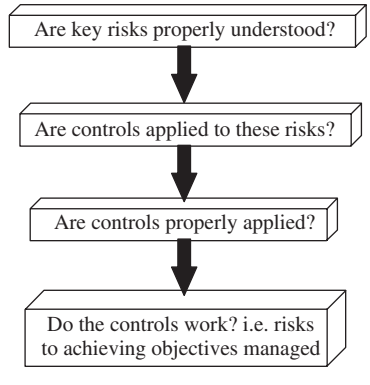


FIGURE 7.7 Key systems audit issues.

The detailed testing routines and comprehensive discussions with management all contribute to better controls. An obsession with the mechanisms of performing the audit and close examination of files and data should not detract from this point. The auditor must at the end of the day be prepared to comment on the systems of internal control and whether these controls guard against all material risks. Moreover, the system for managing risks is dependent on the way the client work team operates. Soft controls are about the way people relate to each other and are motivated (or not). When systems are viewed as dynamic relationships, we can better understand the way control routines are developed and applied. Taking this line, it has been said 'Consider

a business project team. Each person's mood can change from moment to moment. There are many, many different ways they can relate to each other. So a system may have a few parts but a great deal of dynamic complexity. Problems that look simple on the surface may reveal a great deal of dynamic complexity when we probe them.'[7]

Benefits of Systems-based Auditing (SBA)

The well know internal audit guru, Keith Wade (from unpublished course notes from a Masters degree programme, City University Business School, 1991) has argued that SBA has a number of benefits:

1. It is positive and forward looking and considers the future strengths of control systems as opposed to isolating and reporting a series of past errors.
2. It promotes participation by involving the client in explaining the system and its objectives.
3. It promotes professionalism as opposed to churning out auditors who are experts in basic extensive testing routines.
4. It covers everything by being based on the system in operation.
5. It is constructive in seeking to improve systems.
6. It is preventive and views errors in terms of preventing them in the future rather than listing them for management to reprocess.
7. It can be geared into career development as an experienced systems auditor is able to tackle very complicated operations.
8. It promotes respect by requiring the auditor to understand the systems and the client's needs.
9. It develops auditors as experts in control rather than checkers of management.
10. There is unlimited potential to extend systems auditing into all organizational activities.
11. Auditors generally find it more interesting with the emphasis away from testing transactions.
12. It can act as a vital aid to management with long-lasting effects in strengthening controls.
13. It can be a very efficient use of audit resources since it looks for causes of problems and not just the consequential errors.
14. Since it is not error oriented, it is not therefore seen as negative by management.
15. It is systematic, and key areas may be identified and isolated for further attention.
16. It has a wide scope and application and may be used to audit almost anything.

Where internal audit emphasizes testing programmes and probity visits, fraud investigations, compliance inspections, VFM reviews and contract compliance, this is indicative of the transaction auditing approach. The implication is that audit success criteria fall around errors that can be found as opposed to controls that may be improved. This 'error industry' must have weak systems to survive and prosper in total conflict with the systems-based approach. A whole army of checkers can be employed to search and report problems using junior staff with a 'let's catch them' attitude that sets a tone of threat and intimidation. This approach leads to poorly controlled systems that defeat the professional audit objective which is to review and ensure management has installed adequate controls over organizational resources. Figure 7.8 shows how controls when ignored tend to break down, reinforcing the need to test for errors.

An enlightened approach to tackling internal audits is to view the organization as a collection of services that are provided internally or externally. This is based on a number of principles:

1. The organization is viewed as a series of business units where local management is deemed responsible for delivering the defined level and quality of service.

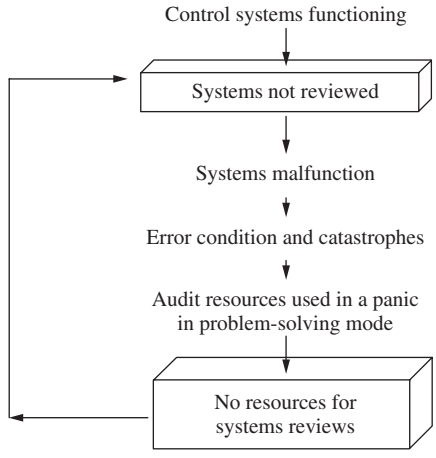


FIGURE 7.8 Transactions approach bottom line – poor systems.

2. The internal control system should be in place to mitigate risks that impact the stated objectives.
3. The various functional support functions including financial, operational, informational and other corporate standards fall under this review if they impact on business objectives.

This approach is epitomized in a local authority where one need only obtain a directory of services such as libraries, child care, schools, refuse collection, highways repairs, housing, sports centres and hundreds of unique services. Each service then becomes an audit unit and subject to audit cover. This is obviously a subjective view of the organization but addresses clearly the problem of defining systems in a precise fashion in line with a high-level approach to service-based systems auditing as in Figure 7.9.

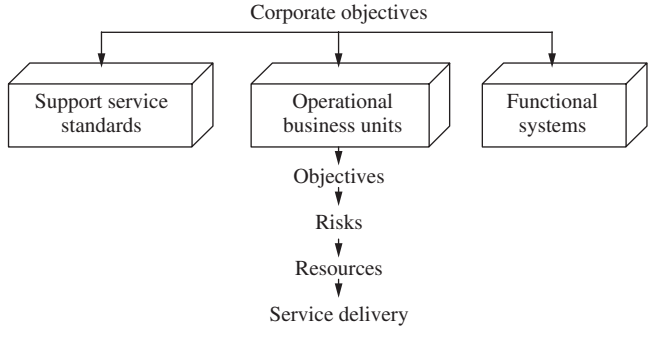


FIGURE 7.9 Risk-based service auditing.

The above approach can be applied as follows:

1. List all services (business units).
2. List support services.
3. Apply risk assessment to these services.

4. Set out audit plans.
5. Audit each service by applying the risk-based systems approach.
6. Perform special investigations into problem areas using resources set aside for consultancy work.

Andy Wynne on Systems

Andy Wynne from the ACCA has prepared a paper for the handbook on systems auditing:

Pre-payment checks, substantive testing or systems audit – what is the most effective role for internal audit? The origins of internal audit are as an internal check on the accuracy and validity of all payments made by an organisation. No payments could be made without them first being reviewed and stamped for payment by the staff of the internal audit section. Internal audit practice now forms a spectrum from this original role of internal audit to systems audit. The latter consists of internal audit reviews of the internal control system with only limited testing of internal controls to ensure that they are actually applied as required. The Combined Code of the London Stock Exchange requires the board of all its listed companies to 'maintain a sound system of internal control to safeguard shareholders' investment' and that 'the directors should . . . conduct a review of the effectiveness of the group's system of internal controls'. In most companies the directors will rely on the company's internal audit function to directly undertake this review of internal control. Many people would agree that the objective of internal audit is to help to ensure that the internal control system of an entity is adequate and effective. Adequate can be construed as meaning fit for purpose, so in the context of internal controls, that the controls are appropriate and that they are actually utilised on a routine basis. The term effectiveness appears to demand more than this and implies an interest in the actual outcome of the controls, for example ensuring that the transactions are actually appropriate, accurate and valid. As a result, if internal audit is to conclude on whether an internal control system is effective it should undertake at least some substantive testing to confirm whether or not the internal controls have operated as expected and thus ensured that the transactions are accurate and valid. In addition, external audit will often rely on internal audit and as part of this reliance, may expect internal audit to undertake a degree of substantive transactions that have been processed by the main financial systems. Pre-payment audit checks (or pre-audit for short) are examinations of payment vouchers and other documents before the associated payments are made. The objective of pre-audit is to ensure that payments made are:

- valid
- necessary and accurate and
- expenditure is in line with the approved budget.

The advantages of pre-audit are said to be that it can help to:

- ensure that all expenditure is necessary and appropriate;
- ensure that all payments are properly authorised before being made;
- ensure that expenditure is in accordance with relevant laws and regulations prevent management fraud;
- reduce the incidence of fraud or irregularity;
- confirm the accuracy of the classification and the coding of expenditure; and
- ensure arithmetical accuracy of the transactions which are checked.

The pre-audit approach to internal audit is found in many African governments, but also in France, Portugal, Spain and many other continental European countries with a legal tradition based on the Napoleonic Code. In these countries, an emphasis is put on the controls that are exercised by a third party organisation, at the centre of government, often an agency of the ministry of finance or that ministry itself. This agency may often be internal audit and until recently this was the approach adopted by The European Commission. Following criticism by the European Parliament of financial management practices within the European Commission, which led to the resignation of the entire Commission in March 1999, a Committee of Independent Experts was established. This Committee concluded that 'the existence of a procedure whereby all transactions must receive the explicit prior approval of a separate financial control service has been a major factor in relieving Commission managers of a sense of personal responsibility for the operations they authorise while doing little or nothing to prevent serious irregularities.' It went on to say that:

> 'whatever the (im)practicalities of these options, the Committee continues to have strong reservations about them on two points of principle. First, *ex ante* checking, whether it be universal or on the basis of sampling, is unlikely to be a cost-effective process: the effort put into checking all transactions is clearly disproportionate, while sampling is unlikely to have sufficient dissuasive effect. The second, and fundamental, principle is that any retention of *ex ante* control runs up against the crucial objection that, *de facto* if not *de jure*, it displaces responsibility for financial regularity from the person actually managing expenditure onto the person approving it. This displacement of responsibility meaning in effect that no-one is ultimately responsible.'

The Committee also recommended that a professional and independent Internal Audit Service should be set up reporting directly to the President of the Commission, that the existing centralised pre-audit function should be dispensed with, and that internal control – as an integrated part of line management – should be decentralised to the Directorates-General in the Commission. The Commission announced in January 2000 that it would accept this recommendation, and a reorganisation of the Commission services began later that year including the establishment of an internal audit service which was independent of the pre-audit or financial control function. The echoes of the pre-audit approach may also be found in some British internal audit sections, especially in local government. Here internal audit may still be expected to review the final accounts of major capital schemes before the final payments are made to the contractors. In contrast, systems audit involves the internal auditors reviewing the adequacy of the system of control and making comments on this rather than on the accuracy or validity of the actual outputs from the system. This systems approach does not necessarily mean that direct substantive testing of transactions is abandoned. However, the 1996 edition of the UK's *Government Internal Audit Manual* stated that substantive testing is 'usually uneconomic' and 'has a limited role to play in systems auditing.' In the aftermath of the collapse of Andersens, resulting from the external audit work at Enron, it may be that there will be increased emphasis on the role of substantive audit work in an external audit. Similarly, there has been some talk of a greater role for internal audit and there may be comparable pressure for internal audit to move back to more direct testing of transactions rather than concentrating its efforts on the internal controls, their adequacy and reliability. The full benefits of internal audit can only be achieved if managers and internal auditors share the same perception of their mutual responsibilities. The view of internal auditors as only compliance auditors may indicate a limited understanding of the roles of modern internal audit and also a lack of understanding of the full range of responsibilities

that managers themselves should have. Internal auditors should work with managers to facilitate the introduction of effective control systems. These systems will include:

- first-order controls to address all significant risks;
- second-order controls to ensure that checks are regularly implemented to ensure that all controls are complied with; and
- third-order controls to ensure that the control procedures are regularly reviewed to ensure they change and adapt in response to a changing risk environment.

Internal auditors should also help to educate managers to ensure that they accept, and understand, the full range of their responsibilities for internal control. These managerial responsibilities should include:

- designing adequate controls;
- ensuring compliance with required controls; and
- regular reviews and revision of internal controls.

The task of the internal auditor is then to review these internal control systems to ensure that managers have adequately fulfilled each of these three sets of responsibilities. Internal auditors should also advise managers on the appropriate controls, compliance checks and review procedures that they should adopt. This is systems audit. An organisation with effective systems audit is more likely to have an effective control system; is less likely to suffer from the range of risks it is exposed to; and is more likely to be successful.

There are several important tasks that the auditor needs to perform to ensure the work is carried out with due professional care. The IIA Attribute Standard 1220.A1 addresses the minimum that must be considered during an audit:

- Extent of work needed to achieve the engagement's objectives;
- Relative complexity, materiality, or significance of matters to which assurance procedures are applied;
- Adequacy and effectiveness of governance, risk management, and control processes;
- Probability of significant errors, fraud, or noncompliance; and
- Cost of assurance in relation to potential benefits.

Business Systems

It is possible to view all business as a series of systems that cover the operations, financial management, support services, processes, partnering arrangements and so on. The business system is illustrated in Figure 7.10.

For simplicity, we have broken the organization down into three types of elements:

1. **Teams –** defined groups of people put together for the purpose of delivering a set objective. For example, an operational team working in production. Internal audit is also one such team.
2. **Processes –** functions that run across an organization such as a complaints procedure or a performance management system.
3. **Projects –** temporary resources assigned to develop a new system or product, for example, a project for designing and implementing a new information system.

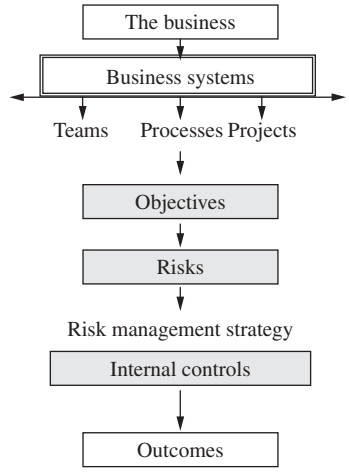


FIGURE 7.10 Risk-based auditing (1).

For all parts of the organization, there would be set objectives, risk and a risk management strategy to address these risks. Hence all such systems throughout the organization may be reviewed by internal audit as set out in Figure 7.11 shows.

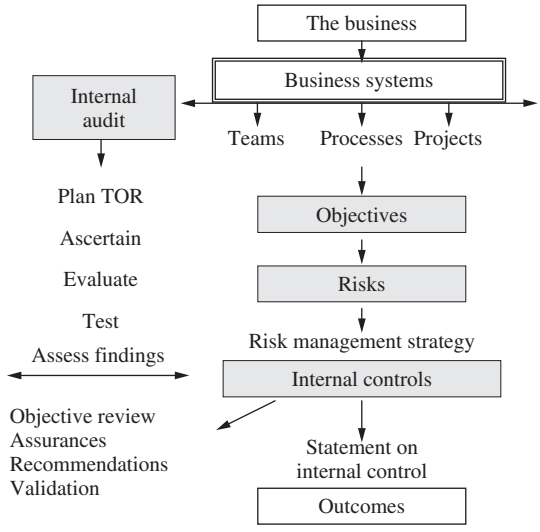


FIGURE 7.11 Risk-based auditing (2).

The internal audit function will examine aspects of the system for managing risks that fall within the agreed upon terms of reference for the audit in question. Audit will ascertain the objectives and system to deliver these objectives, and evaluate whether the controls in place are able to

handle the significant risks that get in the way of achieving the objectives. Testing will determine whether what should be happening is actually happening in practice and provide evidence to support the audit opinion. The products from internal audit are assurances on the way risk is being managed, recommendations for improvement where appropriate and an objective validation of current practices adopted by management. Audit will also consider the feedback loop within the system and how management is able to measure the expected outcomes against the actual results so that the system may be adjusted to ensure improvement. All of this feeds into the statement on internal control and helps ensure the desired outcomes are achieved. We will look at self-assessment (CRSA) in the next section and how this technique may be used for getting better systems to manage risks. Systems auditing is meant to provide an objective review of the system in hand but here we have to issue a word of warning on just how much the internal auditor can achieve, and where the limits lie. Complete objectivity is not possible, even where the auditor is totally impartial, because the audit process can never be removed and separate from the system being audited. This limitation should be appreciated by the auditor and has been neatly described by Joseph O'Connor and Ian McDermott:

> In the final analysis there can never be final objectivity, because you can never stand outside the system of which you are part because you would not exist. Total objectivity is meaningless because there is no observer to describe it. So whether you are being subjective or objective depends on how you define the boundary of the system you are considering.[8]

Soft Systems

Some argue that business systems are so complicated that the auditor needs to adopt more sophisticated ways of analysing them. The standard approach to reviewing a stores system is to isolate the system objective of, say, supply stores to the organization production cycle by accurately specifying goods/services required and purchasing them at minimum cost with due regard to quality and delivery requirements. We may then go on to decide on appropriate control objectives of, say, maintaining low stocks, ensuring no stock-outs, only valid orders being supplied, identifying users' needs and so on. The risks to achieving these control objectives will be ascertained and then current control mechanisms such as a robust information system, stores procedures and inventories, a chief stores manager and so on, will be considered in terms of whether, collectively, they are able to properly manage the defined risks. A soft systems analysis approach would use a form of fuzzy logic to look at the situation with the problem of reconciling low stock holding with the risk of stock-outs and try to build a conceptual model to manage the competing risks. The model will address root causes of problems and motivations and adjust current practice to seek better solutions that make sense to the staff working in the area in question. The soft systems approach will tackle assumptions and positions taken by people's interpretation of the system and try to work through agreed refinements by bringing all interested parties' viewpoints closer together. A systems review that relies on black and white interpretations, which ignores the way people perceive their contribution, will fail to address real issues. Another visit to the art of systems thinking will be useful here as a final word on systems:

> So looking for the effect close to the cause can lead us to false conclusions. We may also be misled by plausible explanations because we tend to look for events that provide our pre-existing models. Remember that in systems thinking the explanation does not lie in different single causes, but in the structure of the system and the relationships within it.[9]

7.2 Control Risk Self-assessment (CRSA)

CRSA is a tool that is used by businesses to promote risk management in teams, projects, through processes and generally throughout the organization. This tool can be used by the executive board, partners, middle management, work teams and, of course, internal audit. In other words, CRSA is both a management tool and audit technique depending on what the CAE wishes to apply to the audit process and the views of the corporate body. In its purest form, CSA integrates business objectives and risks and control processes. Returning to the model of business systems, we illustrate where CRSA fits into the process of managing risks in Figure 7.12.

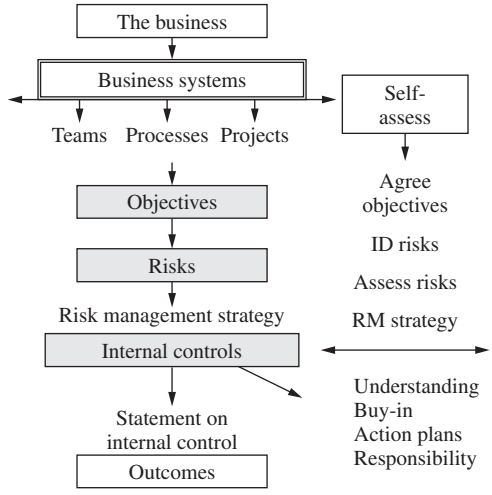


FIGURE 7.12 Risk-based auditing (3).

All business systems have objectives, risks and ways of managing these risks. CRSA is a process for agreeing on the set objectives, identifying the inherent risks that stop one from achieving the objectives and then working out which risks are most significant. Chapter 3 on risk management provides information on the risk management cycle and the way risks may be categorized and assessed. This section simply describes the CRSA technique where it is used in workshop mode. Having isolated the key risks, the team members will go on to refine their strategy for managing the risks, which will tend to focus on internal controls as a main component of the strategy. Note that Chapter 4 deals with internal control in some detail. Allowing the work team (or project team, or representatives from a cross-organization process) to assess their risk management strategy leads to a better understanding of the specific risks and controls in question, to more buy-in as people agree on their approach and to ensuring action plans are realistic. The CRSA approach reinforces the view that the responsibility for controls lies with those that operate them and those that manage the operations.

CRSA and Internal Controls

Some see CRSA workshops as ways of developing contingency plans to protect business interests and for new ventures that are being developed. In fact, many see internal control as mainly

relating to disaster recovery and contingency planning, particularly in response to the threat of terrorist threats. Many risk workshops focus on retaining key staff, and providing back-up arrangements for senior figures or top specialists in the event of an accident or other reasons for their non-availability. Other workshops concentrate on specific projects and ways of managing the risks to larger and more important projects. The traditional view of internal control relates them to measures such as authorization and segregation of duties used as examples in basic accounting systems. One way of analysing this dilemma is to suggest that there are four main types of environments that tend to be subject to risk assessment consisting of process, project, people and preparedness as set out in Figure 7.13.

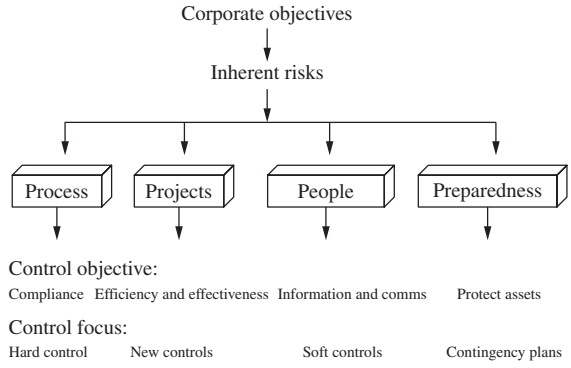


FIGURE 7.13 Types of CRSA.

While in practice there are numerous types of CRSA events, we can suggest four basic approaches:

1. Process Here CRSA is used to review typical controls found in a business process with a view to checking whether the controls are robust and complied with. An example may be a CRSA workshop for the finance team who prepare the group final accounts. The basic controls over information, adjustments, feeder systems, closing accounts, reconciliations and so on will be considered in the light of changing risks (e.g. the risk of financial misstatement) and controls fine-tuned where required. Compliance with these controls also becomes a main consideration. The systems of internal control will tend to revolve around set procedures and information systems, that is, 'hard controls to ensure things are done properly'.

2. Projects These CRSA events will be part of the standard risk assessment and preparation of risk registers that most project management methodologies recommend. Project risk will consist of a combination of the project going wrong and the outcome being poor, late or over budget. Controls will revolve around the way the project is managed and, if this involves a large new venture, an entire set of new controls may be designed and adopted. The focus is on innovation and flexibility and the production of brand new controls that fit the bill. Moreover, risks may also be seen as upside risk that means we take out excessive controls to ensure new opportunities can be exploited.

3. People Some CRSA workshops try to address people issues as the main driver. Here the issues and problems that affect the way the team operates and relates to each other in the pursuit

of business objectives are considered. The idea is to isolate the problems (risks) and solutions (controls) to encourage better performance. A focus on soft controls in terms of people issues is the key factor that drives these types of behavioural workshops. Experienced CRSA proponents like Paul Makosz have promoted the importance of soft controls and have described them as the Sleeping Giant. Moreover, James Roth has suggested that 'you actually have less audit risk when you devote time to evaluating soft controls, because they are more important to controlling an organization than the hard control activities'.[10] In one CRSA-based workshop the background was to identify why the operation was suffering from dysfunction and to:

- identify the current inhibitors that prevent the team from performing to the best of class standard;
- envision how the service could improve in the short, medium and long terms;
- drill down on each of the inhibitors to identify the processes and systems failure or weakness that would prevent or hinder service improvements;
- develop a detailed action plan necessary for the service to improve;
- share best practice wherever possible to aid systems/process improvement.

The workshop sought to assess the risks that could either prevent or accelerate the achievement of the business objectives and considered:

1. how the team sees itself;
2. how the team would like to see itself;
3. what changes are needed to get there.

The findings from the event included the following:

- Significant risks and threats face the operation.
- These risks are not being well managed.
- Control focus is reactive, not proactive.
- Operation is not performing well as a team.
- There are no clearly understood service objectives.
- Many silos are in place based on where staff stand in the hierarchy.
- This has given rise to a blame culture – no collective ownership of problems.
- All staff want to see improvements.
- There are different perceptions of problems from staff, supervisors and managers.

A series of focus groups was set up to tackle problems and help improve the service based on an action plan and a newly agreed on vision for the service.

4. Preparedness This type of workshop is growing in popularity and consists of considering the types of risks that could impact the integrity of the corporate resource, that is, the buildings, the staff, the knowledge, information systems and products or services. The context is the heightened awareness of accidents, sabotage, terrorism and natural disasters that could wipe out a corporate asset overnight. These workshops concentrate on scenario planning and result in risk mitigation strategies, insurance cover and fully resourced contingency plans. Many people now see risk as mainly associated with wide-scale disasters that can stop an organization in its tracks. The emphasis is on protection of assets and containing any potential damage to the continued operation of the business.

It is important to understand which types (or mixture of types) of CRSA events are being targeted. There is little point in getting a finance team to completely redesign their controls, when many are related to set standards and regulators' requirements. There is little scope for talking about standard control routines for a new project team that is making up the rules as they go along, and need new thinking for dealing with new risks. The people workshops depend on 'outing' the people problems that need to be tackled and not designing procedures while ignoring obvious barriers to performance due to poor relationships. Finally, preparedness workshops start with the premise that risks pose real and serious threats to the business and an entire office can be taken out by, for example, a terrorist attack. The success of the CRSA industry is due to the way group/business objectives are used as the lens to focus the energies that are created during the workshop. Many group development events are fun but miss the point, in that they do not really relate to business goals. CRSA is generally positive because anything that brings people closer to understanding and achieving their goals is worthwhile.

Background to CRSA

The IIA issued a perspective on the development of CSA back in 1998 which gave an account of the history of this technique:

> Control self-assessment, a methodology initiated at Gulf Canada in 1987, is a powerful tool that can be used to assess control effectiveness as well as business processes within organisations. The approach that Gulf Canada developed was called the facilitated meeting self-assessment approach. The concept involves gathering management and staff for interviews relating to, and discussion of, specific issues or processes. It is used as a mechanism to assess informal, or soft, controls as well as traditional hard controls. Gulf Canada saw this approach as more effective for CSA purposes than one-to-one audit interviews.[11]

David McNamee has also related the background to CSA:

> Control Self Assessment is usually defined simply as the involvement of management and staff in the assessment of internal controls within their work group. There are a number of ways to accomplish this purpose, from highly interactive workshops based on behavioral models at one end of the spectrum to prepackaged self audit internal control questionnaires on the other end, and a number of techniques in between . . . There are six methods for CSA in use today. The methods range from the most mechanical (least human contact possible) self-administered audit by Internal Control Questionnaires (ICQ) to the most behavioral (most human contact) group workshops. A lot of publicity has been given to the behavioral side of CSA, but there are CSA practitioners getting good results from methods other than group processes.[12]

The IIA's perspective on CSA suggests that the approach chosen should relate to the culture in the organization: 'if the culture is supportive, the IIA recommends facilitated team meetings. In the event a corporate culture does not support a participative CSA approach, questionnaire responses and internal control analysis can enhance the control environment. Internal auditing should be prepared to validate any internal control representations received.'[13]

Back in 1993, people like Tom Oxley were already talking about the new technique:

> What's so good about control and risk self assessment? It forces managers and their staff to think very carefully about their objectives and those of the organisation. It requires them systematically

> to identify, discuss and assess all the risks they face, to decide whether to accept these risks or whether to take action to reduce the level of risk by changing their approach or finding new ways of controlling risk. As a result CRSA places clear responsibility for control with line managers, where it belongs; and the procedures used ensure that managers and their staff are fully involved in, as well as accountable for, controls and risk assessment. This provides a very effective way of identifying and assessing key business risks, and ensures greater commitment to action by management because ideas are not being imposed upon them. Most important of all, the procedure ensures that attention is focused regularly on the real objectives of the organisation. The very process of identifying risks gives managers and staff a much clearer awareness of what they and the organisation are trying to achieve, something lacking in many organisations.[14]

The Internal Audit Role

The IIA has accepted the consulting aspect of helping to establish CRSA in organizations against the background of the internal auditors' expertise in this area. Professional Practices Pamphlet 98–2 makes it clear that 'The IIA recommends using the synergy created by the interaction of the auditor–facilitator and CSA participants to add increased value to the organization through the internal auditing function.'[15]

Some internal auditors feel they need to stand back from the CRSA drive and allow management to assume full responsibility for managing operational risk. Others have thrown themselves into the development and lead from the front under the 'value add' banner. Still others kick-start CRSA in their organizations then stand back and validate the system when it has settled down to some extent. There is no finite solution and much depends on the approach that is adopted. Whatever the final format, the internal auditor must be equipped with the right skills to perform the audit role Note that the next section has a brief account of facilitation skills. There is further advice available from the IIA in the form of Practice Advisory 2120.1 and a pertinent extract on where internal audit fits into the overall equation follows:

> Determine the effectiveness of management's self-assessment processes through observations, direct tests of control and monitoring procedures, testing the accuracy of information used in monitoring activities, and other appropriate techniques.

The positive aspects of CRSA for internal audit have in the past been confirmed by the IIA.UK&Ireland:

- Overall, we believe that Internal Audit have a role to play within any CRSA programme but this role needs to be clearly defined and should in no way detract from its independence and the critical role that it already plays within the organisation. (para. 5.12)
- As line management becomes more proficient in the application of CRSA and the results are accepted by senior management and audit committees, Internal Audit's role and contribution to the organisation may be placed under some scrutiny. The replacement of the Internal Audit function by an established and comprehensive CRSA programme could be seen superficially as an attractive cost saving exercise. This is a mistaken view, as management and other stakeholders are likely to continue to require a level of independent assurance. This is achievable through an effective Internal Audit function. (para. 5.13)[16]

Is There a CRSA Process?

There is obviously no one way of conducting CRSA workshops. In practice, many organizations have interpreted the process to fit the way its people work. Some call them business risk management workshops; some describe them as team-building events based around clarifying team objectives. One large organization used the CRSA process to implement a major change programme that saw regional teams totally reorganized over a short period of some six months. The biggest risk they faced was not achieving the reorganization properly. Another organization could not get their people together in workshops and could only use a questionnaire-based approach with extra time added to group meetings to discuss risk areas. They went on to establish a small number of representative groups to analyse risk across organization-wide processes, and included several stakeholders to ensure all views were considered. One autocratic, head office-based organization simply sent out the results from their corporate risk assessment and told their people to do something similar in their local offices. On the other hand, a more forward-looking entity got their people to embrace the CRSA process and published guidelines for a fully equipped team of facilitators led by the chief risk officer; all equipped with a sophisticated database information system for each risk register and colour-coded risk profiles, along with expensive voting technology for the workshops. In practice it is often better to allow each organization to develop their own solution rather than bring in consultants with the industry-standard package. This results in the adopted approach being developed within the culture that is part of the way the organization works. External consultants should really work alongside the person commissioning the work and pass over skills to employees. When the person charged with setting up the CRSA comes from the finance department, there will tend to be a narrow focus on the concept of risk assessment. One of the best approaches is to locate initial responsibility for setting up the process with the corporate planning officer, so that the link between risk management, planning and performance management is clearly established. If there is a formal board sponsor, close monitoring by the audit committee and a nominated chief risk officer (e.g. from corporate planning), then we are well on the way to the successful implementation of risk management.

One Approach

It is possible to mention one approach to developing CRSA within an organization, although this has to be listed in general terms only (note that the detailed CRSA workshops should be undertaken after having completed staff risk and control awareness seminars as outlined in Chapters 2 and 3):

1. Ensure the designated risk officer is fully acquainted with the theory of corporate governance, risk management and control.
2. Talk to other companies, and people who have experience in developing CRSA in their organizations; or hire a consultant to perform a seminar on the topic.
3. Ensure there is some expertise available in facilitation and related skills.
4. Introduce the CRSA concept – tell the board and audit committee about it and where it fits into the wider aspects of enterprise-wide risk management. If the organization has an annual conference then this would be a good opportunity to launch the initiative.
5. Get the board to endorse a suitable control framework on which to hinge the developing system of risk management. Risk scores may be measured against control models such as

COSO or CoCo using the categories that are suggested in each model. There needs to be a way of scoring or presenting risks such as the Green, Amber and Red measures that some organizations use. Chapter 3 deals with this topic. Some organizations develop a series of control standards in terms of what should be happening, covering areas such as staff ethics, mission and vision, staff competence, performance targets, management information, financial reporting, fraud, operational procedures, supervision and so on (say 10 to 20 standards) and then measure the risk exposures against these standards. Other organizations overlay the risks into the elements of the performance management system such as balanced scorecard or components of the adopted quality models such as European Foundation for Quality Management (EFQM). Control culture organizations tend to want to batten down risks into set control standards so that they may be contained. Organizations with risk-focused cultures tend more to use risk to drive their strategic development models in more innovative ways.

6. Get the board and audit committee to perform their own CRSA workshop at the end of a formal meeting and use the experience and results to drive the initiative.
7. If internal audit is leading the move, then perform a workshop within the internal audit shop. Remember the audit charter should refer to the services that are provided and if this should include CRSA facilitation, then amend the charter accordingly.
8. Secure a board-level sponsor for the programme and start planning. Work through ways of avoiding initiative overload by embedding CRSA into the way the business operates through the planning, communicating, decision-making and performance management systems.
9. Undertake corporate roadshows and introduce the concept of corporate governance reporting and the need for documented risk management. Make sure all key managers understand the CRSA process.
10. Get the right facilities to perform the CRSA workshops. This will include a risk reporting system (based on risk registers), electronic voting software (if this is considered important – some simply use 'Post-it notes' to good effect), suitable accommodation and most important of all – time made available for teams so that they are able to attend the events.
11. Make material available to everyone on the corporate intranet – with useful information, short online exercises and contacts for further information. It may be an idea to post a short guide to CRSA workshops onto the intranet, or have it sent out to key staff.
12. Talk to the manager for the workshop team in question and do some preparation in terms of who should attend and basic logistics. We would probably want between, say, 10 and 15 people per workshop. Decide on the focus, bearing in mind the different approaches and types of CRSA workshops using the process, projects, people or preparedness categories if appropriate.
13. The entire risk assessment system should be part of the enterprise-wide risk management drive and forged around the board-level top 10 risks and the published risk policy. Issue regular board briefings on progress to date.
14. It may be an idea to do a pilot workshop in areas that can result in 'quick wins', without taking on very difficult parts of the business with entrenched problems that would be hard to turn around quickly.
15. Evaluate the results of the pilot with the board sponsor and adjust the approach accordingly.
16. Compile some pre-event material for each participant (e.g. the risk policy – see Chapter 3 – and a few challenging questions) and send it out in advance. Make sure there is a hotline to each participant for any questions. Or contact each participant for a short talk over the phone and discuss the planned event. Most people are apprehensive about team events and feel there is some hidden agenda that is being developed at senior level.

17. Check that the venue is suitable for the participants and that travel, accommodation and practical matters have been dealt with. The entire process must engender positivity all round.
18. Meet and greet the participants and get to know them before the official start of the workshop. Follow-up on anything that has been discussed with them in the pre-course contact stage. The facilitator and scribe should introduce themselves to the group and make it clear what they know about the team and what they do not know. Facilitators need only be experts in getting the best out of people and ensuring that the workshop objectives are both achievable and achieved. Tell the group what is going to happen and how they should contribute.
19. Some believe that workshop rules should be designed by the participants on topics such as everyone should contribute, no dominance from the line manager, stepping outside the box through encouragement from others present, listening, respecting views and not breaking company policy on conduct and diversity, and so on.
20. It may be an idea to get a keynote speaker to introduce the workshop, say a senior manager (or the chief risk officer) or, ideally, the board sponsor (although this person will very often be unavailable). Get the participants to introduce themselves individually and ensure there is a question and answer session at the start.
21. Start the event with clear objectives. This may read something like this: to get the participants to prepare mutually understood (and agreed) objectives, identify and assess risks and then develop risk management strategies determined in conjunction with the existing system of controls and any refinements required; and that the results will form part of a formal risk management reporting system to support the corporate published view on internal controls. Use a prime business objective and, say, five or so supporting objectives. The group may be split into subgroups to deal with these sub-objectives, although it is possible simply to ask the group how they want to play it (so long as the overall workshop objectives are achieved).
22. It may be an idea to perform a brief presentation on corporate governance, risk management and control at the outset. Ideally, this would have already been done at staff awareness seminars on risk management and internal control. Introduce the concept of the risk register.
23. Go through the standard stages of the CRSA process including agreeing objectives, setting the context by getting the group to discuss their performance management, planning and decision making and current change issues facing the area in question. Time may be spent discussing the stages to the decision-making cycle in the work area and also analysing external and internal stakeholders and discussing how their views are accounted for by the team.
24. Get the group to brainstorm operational risks at random and then they can classify them and vote on their relative importance – in terms of impact and likelihood. End up with the top 10 or so risks to achieving business objectives or in not doing more by exploiting new opportunities.
25. May need to perform a short presentation on internal control and what this means in practice, and the difference between hard and soft control. Suitable material may be taken from staff awareness seminars found in Chapter 4.
26. Start the problem-solving stage – this may be done at a separate event (or after a lunch break) so as to reinforce the move from problem identification (risk assessment) to problem solution (risk management).
27. Make the link between objectives, risk, cause and effect clear. Problem solving is about seeing the cause of problems and not just the effects. A simple story can be used to illustrate this idea:

> An osteopath we know told us about one of her patients with severe neck pain. Treating the neck directly had no effect and it took a few weeks to get to the bottom of the trouble.

> The patient had hurt her right big toe. This caused her to walk a little awkwardly, shifting her weight from her painful foot, and this put a slightly different strain on her pelvis. The muscle groups in her back and neck tightened to compensate, and this muscle tightening led to the neck pain.[17]

28. Make sure the workshop is fully documented and agreed on with the resulting action plans giving details of risk owners, particulars of action required, dates and measures to ensure action taken has the required results. These action plans should be incorporated into the planning and decision-making mechanisms to promote integration of CRSA into the business culture.
29. Close the session with a 'people check' – which entails going around the room and asking each person to sum up their experience and what they got from the event and whether they have any further points to add.
30. Risk assessment should be on the agenda at all group meetings, conferences and staff events – whenever there are problems or proposed changes, reference should be made to the current risk register and changes decided on.
31. Roll out the programme through and across the organization and make sure reporting systems make sense and risks are managed in an accelerated manner, which allows the board to know about serious unmitigated risks and that may be monitored urgently or with frequent reports.
32. Make sure the risk register is a live document that is revisited whenever risks materially change and at least several times during the year.
33. Make each workshop a learning process that results not only in the action plan for risk/process owners but also a better use of the workshop format and the way it is facilitated.
34. The best CRSA processes make risk the key driver for business decisions and employee performance appraisal meetings should start with reference to the risk register most closely associated with the employee in question.

The above straightforward procedure does not always work and Mike Pidzamecky has warned about some of the reasons why CSA has failed from an audit perspective:

- Lack of a common body of knowledge and basic process blueprint for all to use.
- Lack of good training and skills development.
- Failure to integrate control models into all audit work.
- Stubborn audit management who could not see beyond traditional audit approaches.[18]

Meanwhile, Andrew Chambers has asked internal auditors to rise to the challenge:

> CRSA, like the quality circles of perhaps a decade ago, has caught the mood of the times. If we dissect it we discover an amalgam of traditional practices often overlaid by modern technology. It may not last forever. It is likely to reinvent itself – perhaps now in the form of enterprise-wide risk management. Despite the pros and cons, it is easier to espouse CRSA in principle than to give it ensuring substance in practice. But then, the effective monitoring of internal control has never been straightforward.[19]

7.3 Facilitation Skills

The CRSA process depends on a good control environment and open communications that engender trust and confidence. People will participate and add to a CRSA workshop if they:

- are committed to the workshop objective;
- have something of value to add;
- believe that their opinion will be appreciated;
- understand the CRSA process and where it fits into the business;
- have confidence in the way the workshop is applied.

Where each of the above aspirations is achieved, there is a good chance that the entire CRSA process will be successful. A few poorly administered workshop events will soon spread the word across the organization that these should be avoided at all costs. Conversely, several positive events will engender a view that they are worthwhile and even enjoyable. There is a lot that can be done in terms of selling the CRSA concept to all employees and ensuring that the workshops are carefully planned and prepared before they go live. One aspect of this preparation is to ensure the workshops are well facilitated and we provide a brief introduction to facilitation skills in this section of the Handbook. The first point to note is that facilitation is not the same as training or managing a group, and this point is reinforced by Lao Tzu who wrote *Tao Ten Ching* in 500 BC:

> A leader is best
> When people barely know that he exists,
> Not so good when people obey and acclaim him,
> Worst when they despise him,
> Fail to honour people,
> They fail to honour you;
> But of a good leader, who talks little,
> when his work is done, his aim fulfilled,
> They will say, 'We did it ourselves.'

A facilitator gets people to do things for themselves. Ideally, the CRSA facilitator should have a good understanding of:

- what makes for a good facilitator;
- groups and how they behave;
- learning styles and how people make progress;
- risk and control concepts;
- different styles of facilitation ranging from passive through to aggressive;
- what could go wrong in a workshop;
- how to make the event successful.

The first three items on the list are discussed below along with a list of features of a successful CRSA workshop.

What Makes a Good Facilitator?

Lois B. Hart in her book *Faultless Facilitation* suggests that facilitation ensures things get done more easily and that the facilitator concentrates on process around group objectives. She lists the attributes of a good facilitator:

Remain neutral	Keep the focus	Be positive
Encourage participation	Protect ideas	Do not evaluate
Suggest methods	Prepare a recorder	Educate the members
Coordinate details	Prepare a report[20]	

This means the facilitator is responsible for helping the group achieve the set objectives for the CRSA workshop. John Heron has described the six dimensions of facilitation:

1. **The planning dimension.** This is the goal-oriented, end-and-means, aspect of facilitation: that is, it is to do with the aims of the group, and what programme it should undertake to fulfil them. The facilitative question here is: how shall the group acquire its objectives and its programme?
2. **The meaning dimension.** This is the cognitive aspect of facilitation: it is to do with participants' understanding of what is going on, with their making sense of experience and with their knowing how to do things and to react to things. The facilitative question is: how shall meaning be given to and found in the experiences and actions of group members?
3. **The confronting dimension.** This is the challenge aspect of facilitation: it is to do with raising consciousness about the group's resistances to and avoidances of things it needs to face and deal with. The facilitative question is: how shall the group's consciousness be raised about these matters?
4. **The feeling dimension.** This is the affective aspect of facilitation: it is to do with the management of feeling within the group. The facilitative question is: how shall the life of feeling within the group be handled?
5. **The structuring dimension.** This is the formal aspect of facilitation: it is to do with methods of learning, with what sort of form is given to experiences within the group and with how they are to be structured. The facilitative question is: how can the group's learning experiences be structured?
6. **The valuing dimension.** This is the integrity aspect of facilitation: it is to do with creating a supportive climate which honours and celebrates the personhood of group members; a climate in which they can be genuine, disclosing their reality as it is, keeping in touch with their true needs and interests. The facilitative question is: how can such a climate of personal value, integrity and respect be created?[21]

Most experts suggest that there should be a facilitator and a scribe, who records the events. For CRSA workshops most of the documentation will revolve around the preparation of the risk register as the objectives, risk, risk rating, examination of existing controls and ensuing action plans are developed by the group. It may be best to use a computer spreadsheet (or database) to compile the necessary information for the risk register. A good facilitator is able to identify the barriers to progress and ways of overcoming these barriers and make strategic interventions when required. The facilitator ensures the group understands the objective and that they are able to keep moving in the right direction. In fact, CRSA is not about preparing the risk register (box ticking) but is more about developing a dialogue where members discuss their views on objectives, things that stop them achieving these objectives and ways of addressing any constraints, that is, a shared understanding is developed to ensure the group members are pulling in the same direction. Where there is misunderstanding among group members and a reluctance to put problems in the spotlight, many of the soft controls (the way people work together) may be poor. The facilitator should be prepared to get the group to challenge anything that stops them from performing. The facilitator does not lead the group, but gets the group to lead itself. The unusual element of the CRSA event is that the facilitator may sometimes need to switch to the

role of trainer and make a brief presentation on corporate governance, risk management and internal control, and also explain the corporate risk policy. If this presentation is done too early on during the workshop, then it may establish a 'listening mode' from the group, which may be hard to switch into 'interactive mode' later on. It really is best to get the presentation done at earlier seminars (or through intranet material) and then ask for any questions during the workshop. Even answering questions can be difficult because it can establish the 'dependency' relationship, where everything the group wants to do is double-checked with the facilitator. This approach will stop the group from progressing independently of the facilitator, who has assumed the mantle of leader. A good facilitator will always offer questions asked of him or her, back to the group and only provide answers where not to do so will stop the group's progress. Humility is an important trait for a good facilitator. This danger is well described by Rosaria Taraschi:

> An intact work group, suddenly faced with the challenge of working as a team, may look to you for answers, support and reinforcement. Although the group may have been functioning well under its old mission, the call to change may leave some members struggling to determine their new roles. Unwittingly, you may become the group's internal expert, coach, change agent, manager of interpersonal difficulties, and so forth. The more you take on, the less likely that the team will gain the skills it needs. The best way to break the cycle is not to let dependency begin. It starts early and gains strength over time.[22]

Learning Styles and How People Make Progress

The CRSA workshop is a means of getting people and teams to understand risks to their business and ensure they are managed properly – and being able to account for this responsibility. The assumption of a defined responsibility creates a change in mindset and underpins a positive control culture throughout the organization. It is a learning process as people learn how to use CRSA as a powerful tool to help them ensure success. A good understanding of the learning dynamic is part of the facilitator's armoury. If the workshops are being run by internal audit staff, then the auditor should think through their expertise on risk and control issues and work out how much of this they can pass on to the group, that is, to get them thinking about their business objectives and risk management strategy. It is less a learning process but more of helping the group to translate what they do into the official speak of the regulator's terminology of corporate accountability, risk management and published statements of internal control. One task of the facilitator is to try to reconcile the visions created by the board, the risk policy and the work teams on what effective risk management means and how it works in practice. Much is related to the set terminology. It is this shared understanding of risk that is so important to effective risk management and being able to appreciate how different perceptions may be tied together. It has been said that:

> We make our mental models partly from our social mores, partly from our culture and partly from the ideas of significant adults in our childhood. The rest we construct and maintain from our experiences in four main ways:
>
> 1. Deletion – We are selective in what we notice.
> 2. Construction – We see something that is not there.
> 3. Distortion – We change our experiences, amplifying some parts and diminishing others.
> 4. Generalisation – Using generalisation, we create our mental models by taking one experience and making it represent a group.[23]

Some facilitators feel that they need to recognize the different types of people who turn up at workshop events and the different ways in which they contribute to its success (or otherwise). Honey and Mumford have developed a learning cycle where people learn from their experiences and plan the next step from this learning. They have also classified different learning styles:

- **Activists –** tend to take direct action. They are enthusiastic and like new challenges and experiences. Activists are less interested in the past or the broader context and are mainly interested in the here and now. They like to have a go and try things out and participate. They also like being the centre of attraction.
- **Reflectors –** think things out in detail before taking action. Reflectors are thoughtful, good listeners and prefer to adopt a low profile. They are prepared to read and listen and welcome the opportunity to repeat a piece of learning.
- **Theorists –** see how things fit into an overall pattern. Theorists are logical and objective 'systems' people who prefer a sequential approach to problems. They are analytical and pay great attention to detail, as well as tending to be perfectionists.
- **Pragmatists –** like to see how things work in practice. Pragmatists enjoy experimenting with new ideas. They are practical, down to earth and like to solve problems and appreciate the opportunity to try out what they have learned/are learning.

If the CRSA workshop is made up of a combination of people with different learning styles, then an understanding of these differences will help the facilitator drive the event better. Another model that provides useful insights into how teams behave has been developed by R. Meredith Belbin. The people who go to make up a management team may assume certain role types as follows:

- **Company worker –** Turns concepts and plans into practical working procedures. Carries out agreed plans systematically and efficiently.
- **Co-ordinator –** Controlling the way in which a team moves towards the group objectives by making the best use of team resources, recognising where the team's strengths and weaknesses lie, and ensuring that the best use is made of each team member's potential.
- **Shaper –** Shaping the way in which team effort is applied; directing attention generally to the setting of objectives and priorities; seeking to impose some shape or pattern on group discussion and on the outcome of group activities.
- **Ideas person –** Advancing new ideas and strategies with special attention to major issues; looking for possible new approaches to the problems with which the group is confronted.
- **Contacts person –** Exploring and reporting on ideas and resources outside the group; creating external contacts that may be useful to the team and conducting any subsequent negotiations.
- **Critic –** Analysing problems and evaluating suggestions so that the team is better placed to take balanced decisions.
- **Team working –** Supporting members in their strengths; underpinning members in their shortcomings; improving communications between members and fostering team spirit generally.
- **Completer–finisher –** Ensuring that the team is protected as far as possible from mistakes of omission and commission; actively searching for aspects of work which need a more than usual degree of attention; and maintaining a sense of urgency within the team.

Some facilitators are so convinced of the importance of understanding these learning and behavioural differences that they ask participants to prepare a pre-course questionnaire designed to isolate their learning style. This information is then used in planning the approach to the event.

Groups and How They Behave

At times, a CRSA facilitator will arrive at a workshop, do the introductions and start the group off perhaps on a simple exercise to get them energized. After a while, the facilitator notices that several participants have pushed their chairs back a little and express negative body language with arms and legs crossed and head turned downwards. They show little interest in getting involved while one group member assumes the role of spokesperson. Meanwhile, another member continually undermines the spokesperson with one-line comments that are never properly explained. The facilitator starts to watch the clock, wishing that the entire event could be cancelled. Much of the above is due to the way groups come together and then decide how to behave. Understanding this point and adapting the facilitation style to suit the group leads to a much better chance of success. The life cycle of groups has been described as consisting of five main stages:

1. Orientation – why are we here?
2. Dissatisfaction – reality does not meet expectations.
3. Resolution – resolve conflicts.
4. Production – tasks are getting done.
5. Termination – group disbands.[24]

Where we can get the workshop group quickly to stage 4 (production), they will take a mature view of the task of getting their risk management strategies agreed upon and documented and can be given a great deal of responsibility. Where the group is stuck at stage 2 (dissatisfaction) they can be considered immature and it becomes more difficult to pass over too much responsibility for the workshop tasks to them. Superimposed over this model is the risk policy (and organizational/group cultures) that will dictate the degree to which staff-based strategies are controlled through tight procedures, set exercises and carefully timed sessions (structured) and the extent to which they allow each group the discretion to set their own agendas and direction (*laissez-faire*). Structured CRSA will tend to be carried out in line with a published guide with set tasks to be completed by the group, whereas *laissez-faire* workshops start with the aim and leave it to the group to decide how they will go about developing the risk registers. Taking the two considerations of degree of group maturity and extent to which workshops are structured/directed, we can derive our own model of facilitation styles as in Figure 7.14.

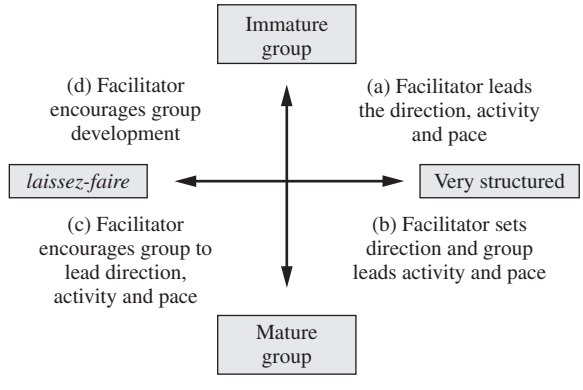


FIGURE 7.14 Facilitation styles.

The facilitation strategies are explained below:

1. For groups that are not yet mature, and where the organizational culture calls for very structured CRSA workshops, the facilitator may lead from the front and set the direction, tasks and so on. For example, the facilitator may inform the group of their section objectives and tell them that they need to brainstorm risks within set categories. Meanwhile, the facilitator may try to get the group to recognize and resolve conflicts so that they can move towards maturity. This type of forum calls for a more aggressive facilitation style where the group is made to work together and given constant encouragement and prompts from the facilitator.

2. Structured workshops mean the facilitator will still set the direction for the group but because they are mature and perform well together, group members are encouraged to work out their activities and pace, so long as they achieve the workshop objective, for example, to arrive at a shared understanding of key risks and a commitment to a defined risk management strategy.

3. The *laissez-faire* approach to workshops can work well with a mature group where the members may discuss and set their own direction, activities and pace – to ensure the workshop meets its aim. The facilitator need only concentrate on the process for working through the stages of risk management and may spend much time sitting down, as group members take charge. Simply sitting down and not making eye contact with the person who is speaking will act to turn the group members' attention to the other members and so allow the facilitator to fade into the background.

4. Where there is little structure to the workshop, and the group is immature, the dimensions change and the facilitator may feel that the biggest risk to the group is located in their lack of progress through the group development stages. Here the facilitator may use force-field analysis to help the group identify barriers to performance and what they need to do to get quickly to the required production stage, or there may be a lot of time devoted to setting ground rules for communicating, working together, respecting views, listening and so on. The group may benefit from a discussion on how decisions are made and encouraged to work through any barriers to making effective decisions. The facilitator may use the *laissez-faire* approach to change the direction of the workshop to focus on team building and development. Moreover, after each session we may stop and check on whether the group is progressing well towards the production stage.

Another way of viewing the workshop process is to suggest that the facilitator may assume a clear presence early on as the idea of operational risk management and the CRSA process is sold to the group. As proceedings progress, the facilitator gradually moves into the background as the group become more confident to work without prompts. Notwithstanding the approach used, the facilitator should always ensure the workshop is challenging to the group members as there is one view that suggests people are reluctant to talk about risks that they cannot control, such as fraud and irregularity. The facilitator should always challenge this reluctance and can ask if 'fraud' can be put up as a potential risk, because there is a lot that can be done to manage this problem, so long as we recognize that it can materialize. The facilitator has a range of tools that can be applied to getting the group to achieve their task, including:

- brief presentations on corporate governance, risk management and internal control;
- clear aims for the workshop;

- open environment where all group members are equal regardless of grade;
- the risk register – a pro forma that shows what needs to be documented;
- the impact/likelihood grid that can be used to demonstrate the significant risks and the link between likelihood and internal controls (controls can help reduce uncertainty);
- list of benefits of effective risk management with practical examples;
- post-it notes that can be used to record views;
- voting – either electronic or otherwise – where group members can record a vote either in public or anonymously;
- techniques for managing consensus through discussion, debate, expert intervention, agreement to disagree, negotiation skills, decision-making criteria, recording dissenting views, statements on the need to arrive at a position, drawing areas of agreement, handing responsibility to the risk owner;
- some knowledge of what other sections are doing about risk management;
- the board's top 10 risks and priorities;
- examples of major problems that have arisen through unmitigated risk;
- the corporate risk policy and direction contained therein;
- warnings about treating risk management as a box-ticking process;
- simple examples that can be further developed;
- models of risk and control (see Chapters 3 and 4);
- techniques for making the event stimulating – such as mini quizzes, exercises in creativity and problem solving, entertaining stories about perceptions of risk and so on;
- material on the big picture of enterprise-wide risk management where the risk registers build into a picture of the entire organization;
- challenging the question assumptions, and reinforcing the view that control rests with everyone;
- building links between views from people in different parts of the organization;
- ability to record workshop events and specific views;
- ability to break the objectives into sub-objectives and work in smaller subgroups if required;
- techniques for dealing with difficult group members – this mainly involves giving them special tasks to encourage their intervention but in a managed fashion;
- flip charts where views can be displayed around the room and referred to when appropriate;
- techniques for moving the group on by limiting time, giving breaks to start a new session, parking points for later discussion (or referral to another venue);
- using views to demonstrate risk appetites;
- placing action points into the risk register;
- demonstration – through the products of a previous workshop undertaken elsewhere;
- empowering the group to choose a method, for example, whether votes should be used or not and how such an exercise should be conducted;
- pace changes – where we check with the group whether to speed things up or slow them down;
- break-out groups to look at particular issues – we can also get the group to work in pairs for a short exercise – for example, list aspects of the operation where there is poor compliance with control standards;
- ability to park the line manager – we can stop this person taking charge and then reintroduce their position towards the end when the action plans are being finalized;
- use of breaks for drinks and other refreshments where energy levels are dropping;

- projecting energy from the facilitator and a belief that the CRSA process is valuable – this is particularly useful where there is some cynicism; remember to write up honest criticisms but with a view to resolving these problems (and follow them up);
- identify points that keep the group energized and use this to encourage participation;
- focus on the task in hand and write up the workshop aims so that anything totally outside the remit can be parked;
- seating arrangements can lead to open engagement – for example, horseshoe with no desks and the possibility to get closer to group members that also allows them to move around freely into subgroups if required;
- dampeners where the action becomes too heated – this may entail a short presentation on points raised and where the corporate position fits in;
- techniques for resuming presence with the group such as standing up, asking questions, giving out tasks, making a clear intervention and assuming a leadership role for a short exercise if required;
- brainstorm techniques – with rules covering idea generation, being non-judgemental, listening skills, time limits, context setting and so on;
- reality checks where we make clear controls, which are never perfect and cost money and time to develop;
- techniques for objective setting where this is an issue – this includes cascading objectives, policy context, links to mission, measurability, time frames, budgets, review mechanisms, business plans, annual reports, authority levels, individual performance targets, communication systems, quality standards, standards of behaviour, group targets, skills, knowledge and attitudes required.

There is a lot the facilitator can do to ensure the success of the CRSA programme and, conversely, there is much that can go wrong where the preparation, buy-in or facilitation is inadequate. Like any initiative, CRSA must be planned and resourced properly and fit neatly into the organizational culture in question for it to have any chance of success.

7.4 Integrating Self-assessment and Audit

The internal auditor may review the CRSA process and the way it is developed and applied in an organization, or the internal auditor may provide a consulting service to help facilitate the CRSA process in a hands-on manner. Since no one can be a judge in their own case, these two approaches can create a potential problem. As mentioned earlier, some audit teams start off the CRSA process, then withdraw to a position of safety and resume the review roles thereafter. Other teams split their staff into audit and consulting services and make sure that the CRSA facilitation aspect of audit is kept separate from the main risk-based systems work. Meanwhile, the IIA Performance Standard 2201 on planning considerations states quite clearly that the internal auditors must consider:

- The objectives of the activity being reviewed and the means by which the activity controls its performance;
- The significant risks to the activity, its objectives, resources, and operations and the means by which the potential impact of risk is kept to an acceptable level;
- The adequacy and effectiveness of the activity's risk management and control processes compared to a relevant control framework or model; and
- The opportunities for making significant improvements to the activity's risk management and control processes.

In other words, the internal auditor should recognize the risk management activity in the area that is being audited and take on board all the effort the client is making to manage risks and establish good controls. This is endorsed by an IIA standard 2201.A1 that makes it clear that:

> When planning an engagement for parties outside the organization, internal auditors must establish a written understanding with them about objectives, scope, respective responsibilities, and other expectations, including restrictions on distribution of the results of the engagement and access to engagement records.

If we produce a complete model of the CRSA/audit process it may look something like the one in Figure 7.15.

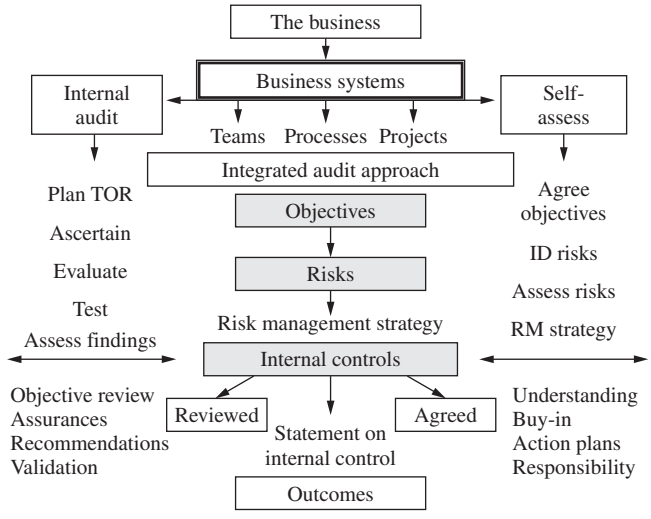


FIGURE 7.15 Risk-based auditing (4).

A mixture of audit objectivity and testing alongside the inside knowledge and commitment from the self-assessment process may create a useful solution. This integrated approach mixes audit with the close involvement of client staff in workshop format to identify risks and help define suitable solutions. Two new boxes are added to the model: reviewed and agreed, that is, the risk management process will have been objectively reviewed by internal audit and also agreed to by the people who actually operate the system, creating many benefits. The best way to illustrate the idea is to give an account of the approach prepared specially for the Handbook by John Watts of Canada Life.

Canada Life – Integrated Audit Approach – Using CSA as an Audit Tool

Canada Life is Canada's oldest Life Company and was founded in 1847. It now has assets of over £23 billion worldwide with some 10 million clients. Canada Life was demutualized in 1999 and has operated in the UK since 1903 with the main UK offices in Potters Bar and the Isle of Man. UK assets are in excess of £6 billion with the 2001 premium income running at over £1300 million. In the UK, stand alone, CSAs (workshop-based using the PDK methodology) have been carried out since 1998 with the results from each workshop being used to provide information for the audit risk assessment process for the future year's audit planning. Additionally,

these CSAs were used to gain an insight into non-process-driven areas where traditional audit methodologies were not wholly appropriate. The concept of 'integrated audits' was developed and run from 2001 onwards, using CSA workshops as an integral part of larger audits where appropriate. There were several reasons why this integrated approach was developed driven by many advantages including:

- Greater coverage of audit universe.
- Enables audit access to new areas.
- Commitment/buy-in from whole department/process owners.
- Addresses 'bigger picture' issues.
- Opportunity to sell audit in new light.
- Common trends/concerns identified.
- Speed.

At the same time, there were several difficulties that had to be overcome:

- Does not cover specific business/process controls.
- Issues raised not reported to Audit Committee nor formally followed up.
- Difficulty in getting 'right' attendees;
- Technology-dependent;
- Standard questions.

The 'integrated audit' using CSA techniques has been used on audits of the major operational processes including senior management team and other areas. Before this, the old traditional audit approach was based on the following key stages:

1. Background research
2. Discussions with management
3. Produce draft key risk and control matrix (KRCM)
4. Further meetings to agree KRCM
5. Test most controls
6. Produce report

Unfortunately, this process tended to lead to:

- Minimal involvement of staff.
- Staff unaware of what Internal Audit are doing.
- Staff not feeling any benefit from the audit.

The new integrated approach differs from this and involves:

1. Background research and presentation
2. Perform CSA workshop with staff
3. Workshop with staff and management to produce KRCM
4. Test key controls
5. Produce report.

In this way, Canada Life was able to add value to the audit product and secure:

- Increased staff understanding of Internal Audit.
- Greater staff involvement in assessing their own processes.
- Staff appreciation of risks and controls.

Turning to the five key stages of the integrated approach, these can be expanded as follows:

1. **Background research and presentation:** We start the audit process by finding out about the area under review by doing the usual desk survey and basic research to isolate general information that helps our understanding of the people, processes and procedures in question. This is followed by a formal PowerPoint presentation to the work team on the audit approach and background to risk management and control. The presentation covers:
   - purpose of internal audit – which is to provide the Board and Management with assurances as to the effectiveness of control over the operation of the business. This entails identifying risks, reviewing control techniques for adequacy and effectiveness then producing a report for management with agreed action if necessary to reduce the risks.
   - comparison of the old and new (integrated) approaches to internal auditing.
   - reasons why the approach was changed – i.e. to provide a more comprehensive and detailed coverage of the business area, increase/derive mutual benefits.
   - reinforce the view that the person who performs the task understands it better than anyone else – i.e. the staff themselves!
   - risk management and the whole ambit of determining objectives, inherent risk and risk management strategies.
   - the CoCo model of control and how this creates a dynamic framework for developing and reviewing internal controls.
   - the difference between hard controls (such as authorizing signatures, documentation, limits, reconciliations, checklists, supervision and exception) and soft controls like teamwork, leadership, morale, training and communication.
   - risk categories – market risk, credit risk, insurance risk, liquidity risk, operational risk, legal and regulatory risk and strategic/corporate risk.
   - the way risk assessments and controls work are swept up into Canada Life's key risk and control matrix format as part of the company's enterprise-wide risk management and corporate governance reporting arrangements. The KRCM summarizes all the inherent risks to which an area or process is subjected and the potential implications/consequences, the controls in place which seek to manage those risks and an assessment of how effective the controls are working.
   - close the presentation and ask for any questions.
2. **Perform CSA workshop with staff:** Having 'sold' the value of the audit approach, risk management and internal controls, we then get the team together to isolate their key risks before we start the audit proper. This entails two separate parts of the day's workshop. The first part incorporates a 'Post-it' note exercise to gain an assessment of the team's view on the current obstacles preventing, and current strengths assisting, the team meeting its objectives. Part two is asking them a series of standard questions (asked at every session) based around the CoCo model on purpose, commitment, capability and learning to gain a more complete picture of the issues within the area. The CSA process is interactive, uses electronic voting technology throughout and captures the team's comments on a laptop. All voting and comments captured are displayed to and agreed with the team in the session.
3. **Workshop with staff and management to produce KRCM:** This next stage is designed to build the key risk and control matrix as a main part of the assurance reporting. The aim here is to complete the KRCM in the most efficient but effective manner by having all, or a realistic representation of, key staff involved in the department/process, involved in this workshop at the same time. This approach avoids the constant updating of the KRCM with different views/comments and should facilitate the production of an accurate and agreed KRCM in one session.
4. **Test key controls:** One difference with CSA as a management process is that there is no testing carried out during the workshops. Using CSA as an audit tool, we are able to

focus the testing strategy towards the high risk areas and key controls. This is important in risk-based auditing – as teams identify and assess their operational risks and then work out how to manage them. While we build on this work by directing our audit tests to areas they have identified as high risk aspects of the operation. The testing undertaken will take into account all key areas of risk identified in the CSA and the KRCM workshops and will seek to confirm the existence and effective operation of any mitigating controls identified within the process.

5. **Produce report:** The report is more of an agreed action plan that comes from the combined efforts of clients and the auditors working together with the common aim of improving the risk management process and the underlying control environment. Major issues identified within the CSA workshops are included in the final audit report. They are therefore formally reported to senior management and the audit committee and are part of the monthly follow-up of outstanding audit issues.

Our integrated approach to our more significant audits combines the assurance and consulting role of internal auditing. In this way, we are able to encourage (and equip) client managers and their staff to develop good systems of risk management and underlying internal controls. We are also able to direct our audit towards areas of high risk, and independently test and explore any areas of concern. Meanwhile, we work with operational work teams and Risk Management to improve business performance at Canada Life.

Integrated audits can provide an interesting way of refining the audit process, adding more value to the audit product. It has been suggested that:

> The prudent corporate approach is not to see CRSA as an alternative to internal audit, but rather to co-ordinate CRSA with the internal audit process and see them as complementary ways of assessing risk and control. Conventional internal auditing has the advantage that audit findings are supported by evidence which internal auditing standards require to be contained within the records of the audit engagement. 'Evidence' in the CRSA programmes is, in the main, vested in the knowledge and experience which the participants bring to the CRSA workshops – which has its own advantage as their 'know-how' is likely to exceed that which can be acquired by a sole internal auditor or by an internal audit team during the brief fieldwork of an audit assignment.[25]

7.5 Fraud Investigations

Fraud is big business and the real scale may be unknown. CIPFA has defined three categories of fraud:

a) those which are known and recorded publicly;
b) those which are known only within organisations and which will not be brought into the public arena; and
c) those which are, as yet, undiscovered.[26]

It is the last category that is most worrying – frauds that have not yet come to the surface. Frauds arise when 'things go wrong' and this has implications for the system of internal control. Because it is so sensitive, management becomes desperate to investigate and solve alleged frauds. They need as much support as possible and generally turn to internal audit for guidance. The audit function should have extensive knowledge of frauds and how they are investigated, if the service is provided by them as opposed to being the responsibility of a specialist fraud team. This section

summarizes the minimum knowledge for the auditor. A survey conducted by Management Today and KPMG Forensic Accounting suggests that:

> 'unethical behaviour' – from pilfering pens and surfing the net while at work to outright fraud – remains endemic in the British workplace. And it runs from the boardroom to the shop floor. Although most managers have a fundamentally ethical approach to business, a majority are aware of dishonest conduct in the workplace but accept it as inevitable. They simply cost it into operations and don't blow the whistle on offenders.[27]

Another survey involving senior executives from 10,000 organizations representing more than 30 different industries in 15 countries concluded that (extracts only):

- 82% of all known frauds perpetrated by employees.
- A third of these committed by management.
- Greater propensity among managers to perpetrate acts of fraud.
- Organizations which had not performed fraud vulnerability reviews were almost two-thirds more likely to have suffered a fraud within the previous 12 months.
- 40% of participants who thought their organization was vulnerable to fraud indicated that their organization lacked a specific policy with respect to reporting fraud.
- 80% of respondents who had used forensic accountants expressed their satisfaction with the work performed.
- Almost two-thirds of participating organisations had been defrauded in the last 12 months.
- Almost one in ten had suffered more than 50 frauds.[28]

The ACFE's 2002 Report to the Nation estimated that for the US, 6% of revenues ($600 billion) was lost in 2002 as a result of occupational fraud and abuse. The report concluded:

- occupational fraud and abuse is a serious problem for organisations;
- cash is the asset most frequently targeted by dishonest employees;
- most occupational frauds are ongoing;
- the most costly frauds are committed by well-educated senior male executives;
- internal controls are a deterrent to occupational fraud;
- workplace conditions affect the rate of fraud within an organisation;
- the single most effective means of detecting occupational fraud is through tips and complaints;
- audits and other anti-fraud measures are effective in reducing the cost of occupational fraud and abuse, and
- employee education is an important aspect of preventing occupational fraud and abuse.

The 2008 Report to the Nation provided the following worrying conclusion:

> Participants in our survey estimated that U.S. organizations lose 7% of their annual revenues to fraud. Applied to the projected 2008 United States Gross Domestic Product, this 7% figure translates to approximately $994 billion in fraud losses.

It is notoriously difficult to obtain reliable statistics on employee fraud. CIFAS (the UK's fraud prevention service – www.cifas.org.uk) make clear that not all fraud cases make it to court, so figures on court cases can be unreliable. A CIFAS research project suggested that UK company fraud stood at £40 million pa involving over 1,500 staff dismissals although they admit that this figure could be much higher.

What is at Risk?

An analysis of theft and fraud in government departments for 2001 reported that some 51% of government bodies reported no frauds, while the other 49% reported 539 cases to a value of £1.6 million. The types of fraud reported included:

Types of fraud:	**Number**	**Value**
Fraudulent encashment of payable instruments	1%	1%
Misappropriation of cash	14%	4%
Theft of assets	33%	25%
Works services projects	2%	3%
Travel and subsistence	12%	8%
Instruments of payment received on false documents	6%	49%
False claims for hours worked	11%	3%
Other	21%	7%

Some of the main risk areas for employee fraud include:

Debtors	Cash
Payroll	Large capital contracts
Revenue contracts	Major computer acquisitions
Computer access	Attractive portable items (e.g. laptops)
Public sector benefits	Government grants
Expenses	Stock
Cheques drawn	Creditors and payments
Mortgages	Pensions
Petty cash	Recruitment references
Overtime and employee claims	Confidential information
Subsidy claims	Credit cards
Computer memory chips	Corporate knowledge
Employee bonus schemes	Procurement

Defining Fraud

The IIA define fraud as:

> Any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage.

The ACFE define occupational fraud as: 'The use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets.'[29]

The UK's 2006 Fraud Act was designed to address the growing threat of fraud by making provision for, and in connection with, criminal liability for fraud and obtaining services dishonestly through:

1. false representation
2. failing to disclose information
3. abuse of position.

The act also creates new offences of possession and making or supplying articles for use in frauds, and the new offence of obtaining services dishonestly. The offence of fraudulent trading is extended to sole traders.

Fraud can take place where an innocent error has gone undetected so that the ability to breach a system's security becomes evident. Once a member of staff spots a system weakness, it can be used to perpetrate fraud. This weakness may consist of unclear procedures covering access privileges to a computerized system where there is little distinction between authorized and unauthorized work. Some argue that this equation is important:

$$\text{Motive} + \text{Means} + \text{Oppurtunity} = \text{Fraud}$$

Here the person with

a reason	(say paying large amounts of alimony),
ability	(in that the technical or other skills are present) and
access	(possibly with the chance to conceal the fraudulent act)

may be prepared to perpetrate fraud against an organization. Fraud may be perpetrated internally by employees or externally by third parties. It may consist of a conspiracy between outsiders and an employee, as with many contract frauds. Fraud may:

Be complicated It may be perpetrated by someone with particular expertise in an area. An individual's actions may appear normal to an outsider with no experience. An example is when fuel is transported; it expands and would appear to be of greater volume. The mere act of selling fuel based on its value after transportation may not be viewed as an actual fraud.

Be simple Some frauds may be very simple and involve basic adjustments to documents. One fraud was based on the use of Tipp-Ex erasing fluid on a photocopied document that fooled a bank into parting with £6.7 million, via a transfer to an overseas bank.

Be one-off or continuous A criminal may steal a cheque, forge the amount to make it greater in value and then pay it into a specially opened bank account. The offender will hope to be gone before the loss is discovered. An employee may fabricate petty cash claims of reasonable value over a long period of time such that the aggregate amount becomes material. In the first case, time is an essential factor to catch the culprit. In the second case a painstaking exercise may be required to put together all fraudulent claims so that the clear weight of evidence accumulates throughout the investigation.

Be carefully planned A fraud may be planned over a long period where all loopholes are considered before it is carried out. It may be that in the normal course of events it will not be uncovered and only comes to light when additional checks are made. An outsider will have a great deal of difficulty in uncovering these types of frauds without being tipped off.

Involve regular amounts Some frauds are used to top up salaries and involve regular amounts. Misappropriation of stores may fit into this category so that each theft is unnoticed. The main problem is that management information, may have been for some time, based on deflated figures and so give no clues to any under declaration. The sums received may then appear to be what is expected and all sides are content. Some see this as a perk of the job. Local traders may prefer

to pay refuse collectors cash sums rather than official (and more expensive) accounts raised by the local authority for the removal of trade refuse. On a grander scale, the Bank of Credit and Commerce International scandal of the 1990s exposed an organization that was involved in fraud on a day-to-day basis.

Be perpetrated by senior officers The scenario of the long-serving senior manager who has a dislike for the internal auditor is seen in many departments. Answers that do not make sense may be provided to a junior auditor who feels unable to challenge the manager. The manager may then insist that 'getting things done' is more important than complying with official procedures and this argument may be used time and time again. If this employee does perform well, then superiors may not delve too deeply into their activities and control breaks down. Senior staff have greater access privileges and may be able to authorize discretionary transactions without challenge. The view that all senior staff are naturally trustworthy is not always correct. Frauds perpetrated by the late Robert Maxwell were based around an organization where staff felt they could not challenge him.

Involve large amounts One type of fraud that is high profile relates to Euro subsidies. In the past, the European Commission has disallowed over £1 billion as expenditure improperly incurred.

The Four Components

Fraud is an act of deceit to gain advantage or property of another with four main components:

1. **Motive.** There should be a motive for the fraud. This may be that the employee is dissatisfied or is in financial difficulties. In the case of non-employees, there should be a reason why the fraud is perpetrated. Good human resource management keeps employees satisfied and lowers non-financial motives for engaging in frauds.
2. **Attraction.** The gain or advantage secured must have an attraction for the perpetrator. This varies and may provide a gain for an associated person, for example, a mortgage applicant.
3. **Opportunity.** There must be adequate opportunity. Someone may wish to defraud an organization and know exactly what is to be gained, but with no opportunity, it may never occur. Preventive control should be used to guard against the possibility of fraud by reducing opportunities. In fact, a report by the University of Nottingham Business School (commissioned by Business Defence Europe) based on a study of 200 firms, claims that middle managers are particularly likely to defraud because they have an in-depth knowledge of how their firms work and know how to cover their tracks.[30]
4. **Concealment.** In contrast to theft, fraud has an element of concealment. It can be by false accounting which is a criminal offence. This makes it difficult to uncover and allows the fraud to be repeated.

Mort Dittenhofer has used three main factors, pressure, opportunity and integrity, to assess the likelihood of fraud:

PRESSURE	OPPORTUNITY	INTEGRITY	POSSIBLE RESULTS
HIGH	HIGH	LOW	FRAUD
HIGH	HIGH	HIGH	TEMPTATION
LOW	HIGH	HIGH	NO FRAUD
LOW	LOW	HIGH	NO FRAUD
HIGH	LOW	HIGH	TEMPTATION[31]

The causes of fraud will vary but in terms of reported government fraud the causes of fraud have been listed as:

Causes:	Number	Value
Absence of proper control	24%	14%
Lack of separation of duties	1%	1%
Collusion with persons outside department	8%	31%
Failure to observe control procedures	50%	48%
Collusion within the department	3%	4%
Other	3%	2%[32]

Types of Fraud

There is no legal definition of fraud. The fraud may be carried out by insiders or outsiders and an organization may carry out fraud by, say, overstating its earnings. Acts associated with fraud are:

Theft This includes obtaining property by deception and false accounting. It is defined as 'Dishonestly appropriating property belonging to another with the intention of permanently depriving the other of it'. The Theft Act 1968, section 17 covers false accounting which may be the most common charge of fraud:

> Where a person dishonestly with a view to gain for himself or another or with the intent to cause loss to another (a) destroys, defaces, conceals or falsifies any account or any record or document made or required for any accounting purposes; or (b) in furnishing information for any purposes, produces or makes use of any such record or document as aforesaid, which to his knowledge is or may be misleading, false or deceptive in a material way.

The Theft Act 1968, section 22 covers stolen goods and provides that 'A person handles stolen goods if (otherwise than in the course of stealing) knowingly or believing them to be stolen he dishonestly receives the goods, or dishonestly undertakes or assists in their retention, removal, disposal or realization by or for the benefit of another person, or if he arranges to do so.'

Bribery and corruption The Prevention of Corruption Acts 1889 to 1916 apply to local government and provide that 'any money, gift or consideration paid or received shall be deemed to have been paid or received corruptly as an inducement or reward unless the contrary is proved.' The Local Government Act 1972, section 117(2) provides that an officer should not under 'colour of his office or employment' accept any fee or reward whatsoever other than his proper remuneration. The Local Government Act 1972, section 117(1) states that:

> If it comes to the knowledge of any officer employed, whether under this act or any other enactment, by a local authority that a pecuniary interest, whether direct or indirect (not being a contract to which he is himself a party), has been, or is proposed to be, entered into by the authority or any committee thereof, he shall as soon as practicable give notice in writing to the authority of the fact that he is interested therein.

The Audit Commission defines corruption as 'the offering, giving, soliciting or acceptance of an inducement or reward which may influence the actions taken by the authority.'

Forgery 'A person is guilty of forgery if he makes a false instrument with the intention that he or another shall use it to induce someone to accept it as genuine and by reason of so accepting it, to do, or not to do some act to his own or some other person's prejudice.'

Conspiracy This involves the unlawful agreement by two or more persons to carry out an unlawful common purpose or a lawful common purpose by unlawful means. This would cover collusion to override internal controls.

There are other actions that fall under the generic category of fraud, including:

- perjury
- concealment (of information)
- fraudulent trading (e.g. inability to pay creditors)
- conversion (fraudulently endorsing a cheque)
- financial misstatement.

Unauthorized removal and breach of internal procedures may also be investigated but these are seen as internal disciplinary matters with no criminal implications. Cybercrime is a growing problem and a survey by the Confederation of British Industry placed types of cybercrime in order of perceived threats:

Viruses	Hacking
Illegal database access	Adverse comments on the Internet
Intellectual property infringement	Legal liability issues
Distorted versions of website	Credit card fraud
Securities and financial fraud	Money laundering

The survey reported that the main perpetrators were hackers (45%), former employees (13%) and current employees (11%).[33]

The Regulation of Investigatory Powers Act 2000 created a new criminal offence and a tort of unlawful interception of communication being transmitted by certain means. Certain transmissions can be intercepted if authorized and the Secretary of State may issue interception warrants for certain purposes and to require the disclosure of an encryption key. Electronic signatures consist of a public encryption key linked to a private key, so messages are secure as long as the authorized user transmits the message. The Electronic Communications Act 2000 allows this device to be submitted in court as evidence, as would a traditional signature. The Act contains arrangements for the Secretary of State to maintain a register of approved cryptography providers. Money laundering is also a growing concern and it is an offence:

- for any person to provide assistance to a criminal to retain, conceal or invest funds if that person knows or suspects that the funds are the proceeds of crime; the definition of crime for money laundering purposes is now very wide and includes the proceeds of anything from theft to tax evasion;
- to prejudice a money laundering investigation by informing any third party that an investigation is underway;
- not to report a suspicion of laundering relating to drugs or terrorism.

Financial services firms have additional requirements to verify the identity of customers and to identify suspicious transactions.[34]

Meanwhile, the ACFE have three basic categories of occupational fraud:

1. asset misappropriations. 86% of cases and 90% involve the theft of cash.
2. corruption – wrongful use of influence eg kickbacks.
3. fraudulent statements – falsification.[35]

Indicators of Fraud

Frauds are normally found through luck or third-party information while some are discovered during audit reviews, or through controls or by line management. The following are lindicators of fraud:

- Strange trends are exhibited where comparative figures move in an unexplained fashion. For example, spending patterns on attractive portable items may suddenly increase over the Christmas season or unexplained drops in income may appear on income returns. It is not unknown for spending against revenue budgets to increase towards the end of the financial year.
- Rewritten and/or amended documents may be evidence of unauthorized alteration to cover up fraud.
- Missing documents may signal a fraud where items are sensitive such as unused cheques or order forms. Computers can print out missing items by isolating gaps in sequential numbering.
- Tipp-Ex (erasing fluid) applied to documents may indicate unauthorized alterations. This can be readily used with photocopies to create distorted file documents. We can normally see the original entries by holding up the reverse side of the original document against the light.
- Photocopies substituted for originals can be readily tampered with since the photocopy may make it impossible to uncover alterations to the original.
- Complaints from suppliers that do not tie in with the records should alert one to a potential problem. So if a supplier claims that their payment was not received, although the cheque has been cashed, this may mean that the money has been diverted to the wrong account.
- Social habits of staff are sometimes used as an example of a fraud indicator particularly where they appear to be living beyond their means. This should be used carefully since it is not uncommon for people to have more than one source of income. Some fraudsters arrive at work very early in the morning or stay late at night when they may alter records unobserved. Others have obsessive jealousy over their work and resent any intrusion or take very little annual leave at all.
- Other unusual situations arise such as excessive voids, write-offs, unauthorized personnel with access, unrealistic contract prices, persons being too cooperative, vendors increasing invoices, supporting records unavailable, non-serial-numbered documents, one person in control, willingness to settle claims, excessive write-offs, lots of journals, key staff on low pay, no anti-fraud policy, poor understanding of controls, poor compliance history, poor relations between audit and management, little management supervision, poor accountabilities, poor recruitment screening, low employee morale, employees working unsocial hours without supervision, no security consciousness, large cash transactions, complex transactions, new accounting system, confirmation letters not sent, contracts with poor specifications, no tenders, changes in prices, post-tender negotiations, out-of-balance general ledger, excessive purchases and travel and subsistence, ghost employees, inventory shrinkage, increased scrap, large one-off payments, excessive employee overtime, unusual invoices, strange ratios and trends.

Many indicators go unnoticed and the problem arises when, after a fraud has been uncovered, there are criticisms that there was obviously something wrong that should have been spotted.

There are employees who are alert to these signs and as long as the organization promotes alert behaviour this becomes an additional control. The only real remedy is effective controls.

Fraud Detection

The ACFE 2002 Report to the Nation suggests that the main sources of detection in the US (percentage shown in brackets) come from:

1. tip from employees (26%)
2. by accident (19%)
3. internal audit (18%)
4. internal control (15%)
5. external audit (11%)
6. tip from customer (9%)
7. anonymous tip (6%)
8. tip from vendor (5%)
9. notification by law enforcement (2%).[36]

The British Government Fraud Report has a different list of means of discovery:

Detection method:	**Number**	**Value**
Normal operations of control procedures	59%	56%
Internal audit	1%	1%
Suspicion	4%	2%
Accident	4%	2%
Information from third party	30%	39%
External audit	1%	1%
Confession	1%	1%
Other	1%	1%[37]

Defining Roles in an Organization

In terms of fraud detection, there is a clear difference between management and internal audit's roles:

1. Management and the internal audit activity have differing roles with respect to fraud detection.
2. Management has responsibility to establish and maintain an effective control system at a reasonable cost.
3. A well-designed internal control system should not be conducive to fraud. Tests conducted by auditors, along with reasonable controls established by management, improve the likelihood that any existing fraud indicators will be detected and considered for further investigation.

Before we consider individual roles in more detail, we can refer to previous guidance from the IIA.UK&Ireland, which suggests that all organizations need to identify the risk of fraud and its impact on the organization, and as such should:

- set the tone from the top by having a policy that fraud will not be tolerated and fraudsters will be prosecuted;
- have a fraud mitigation strategy to detect and deter would be fraudsters;
- have a fraud response plan setting out exactly what steps to take if a fraud is reported or detected.

Within this broad remit, individual roles in respect of fraud include the following:

Management Management is directly responsible for ensuring all actual or suspected frauds and irregularities are investigated and resolved. This is achieved by recognizing the risks involved and establishing suitable controls. Management is responsible for making sure fraud does not happen. The European Confederation of Institutes of Internal Auditing (ECIIA) has said that:

> Directors, managers and all employees should be trained in fraud awareness. Internal auditors should receive wider training in fraud prevention and detection and be required to maintain an up to date knowledge base of this discipline. (para. 1.4)
>
> The information available to the board, the audit committee and senior management in respect of all internal control operations – and particularly those controls designed to prevent fraud – will be enhanced where an internal auditing function is in place, properly resourced and reporting at a high level. (para. 1.5)[38]

Internal audit Internal audit is responsible for reviewing the way systems minimize the risk of waste, breach of procedure, poor VFM and fraud. Within the audit terms of reference, under the scope of audit, appears the issue of safeguarding the organization's assets. The question then arises as to whether this is in terms of reviewing controls over assets or examining whether they are properly accounted for and taking action if not. The first approach is systems based, while the latter is geared into transactions testing or is probity based. A SBA approach provides a more effective use of audit resources but the problem is that management does have an expectation that audit will help uncover major error/irregularity. Legislators also tend to hold the view that audit will keep a check on management. In some organizations, the audit role and the fraud investigators' role are separated, and in other audit departments, a great deal of time is spent on frauds as opposed to planned systems reviews. The extreme occurs where cases are referred wholesale to internal audit. They are investigated and audit reports them to the police in addition to initiating any resultant disciplinary hearing against the employee in question. The organization should negotiate the audit role in respect of frauds. Principles to be applied are:

1. The audit charter should establish the audit role in frauds.
2. The organization should define a clear policy on fraud and if this involves internal audit then it should say so. It may be that all frauds are reported in the first instance to internal audit.
3. Within the organizational policies, internal audit should establish a service-level agreement that will describe the role in frauds. This should be agreed to by the audit committee.
4. Whatever is agreed, it is clear that management is wholly responsible for investigating and resolving their frauds and any internal audit involvement is, in reality, consultancy work.
5. The most effective model is where management resolves its own frauds, while internal audit provides an advisory role. If properly directed, management can use its close knowledge of the affected area to speed up the investigation, while audit has a learning curve before the work can be performed. If management is kept out of investigations because of a lack of skills, then it is being deprived of this experience that once acquired will enable it to deal with fraud. The main exception is where the report is going to an outside body or the nature of the fraud implicates all tiers of management and an independent investigation is required.
6. Executive decisions should be made by management who should implement action required to solve the fraud. Even where audit carries out investigatory work, it is essential that management issues any resulting instructions.
7. Where audit investigates the fraud they should be careful not to become manipulated by management. If it is clear that, because of their behaviour, the managers whom audit is

working for are partly responsible for the irregularity, then audit needs to clear a reporting line to the next tier of management. The party under suspicion must be given the full opportunity to explain their actions and management should not apply oppression. Managers have been known to dismiss innocent staff and pay them any consequential compensation at the employment tribunal.

8. Once a fraud is resolved, audit must ensure that management recognizes its responsibilities to close internal control loopholes. One must be careful that audit is not used to regularly discipline staff because management cannot be bothered to install effective internal controls.
9. In terms of fraud detection, IIA Attribute Standard 1210.A2 makes it clear that '*Internal auditors must have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization, but are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud*.'

The IIA.UK&Ireland's old Fraud Position Statement argues that the roles that internal audit could undertake include the following:

- Reviewing fraud prevention and detection processes put in place by management;
- Assisting management to improve those processes;
- Leading investigations where necessary;
- Liaison with the police;
- Dealing with whistleblowers.

For a pan-European view we can return to the ECIIA, whose position paper on fraud makes it clear that:

- Internal auditing can make a significant contribution to fraud prevention by undertaking its primary role of providing management with (1) opinions on internal control effectiveness, (2) recommendations for control improvement and (3) information on leading-edge techniques for fraud detection and risk assessment. (para. 1.6)
- Internal auditing can provide the organisation with a secure environment for employees to raise concerns when it is perceived that these concerns are not being addressed by line managers. A confidential process, based on best practice, can be put in place by internal auditors which can formally 'leapfrog' the hierarchical structure and directly inform the board and its audit committee. (para. 1.7)
- Internal auditing can bring its skills of investigation, analysis and evidence gathering to those circumstances where fraud is suspected. Operating under a board-approved Charter, internal audit can investigate and secure evidence to the point where a report can be made to external authorities – if that is appropriate – with a reasonable chance of a subsequent successful prosecution. (para. 1.8)[39]

The internal auditor needs to take care when carrying out the audit task and take into consideration the risk of fraud. The IIA's Attribute Standard 1220.A1 reinforces the need to exercise due professional care by considering the:

- Extent of work needed to achieve the engagement's objectives;
- Relative complexity, materiality, or significance of matters to which assurance procedures are applied;
- Adequacy and effectiveness of governance, risk management, and control processes;

- Probability of significant errors, fraud, or noncompliance; and
- Cost of assurance in relation to potential benefits.

The external auditor The external auditor must ensure that management has taken reasonable steps to control fraud, and where this is insufficient, it may be referred to in a management letter. The external auditor will ensure that fraud in terms of the possibility of material misstatement of the accounts is considered when planning the audit and reviewing internal controls. They will follow-up indicators of fraud and report the results to management and the external auditor may be asked to advise management on the prevention of fraud. The *CFE Fraud Examiners Manual* includes a survey of large accounting firms' auditors' potential warning signs of financial-statement fraud – ranked in order of importance:

- Managers have lied to the auditors or have been overly evasive in response to audit inquiries.
- The auditor's experience with management indicates a degree of dishonesty.
- Management places undue emphasis on meeting earnings projections or other quantitative targets.
- Management has engaged in frequent disputes with auditors, particularly about aggressive application of accounting principles that increase earnings.
- The client has engaged in opinion shopping.
- Management attitude toward financial reporting is unduly aggressive.
- The client has a weak control environment.
- A substantial portion of management compensation depends on meeting quantified targets.
- Management displays significant disrespect for regulatory bodies.
- Management's operating and financial decisions are dominated by a single person or a few persons acting in concert.
- Client managers display a hostile attitude towards the auditors.
- Management displays a propensity to take undue risks.
- There are frequent and significant difficult-to-audit transactions.
- Key managers are considered highly unreasonable.
- The client's organization is decentralized without adequate monitoring.
- Management and/or key accounting personnel turnover is high.
- Client personnel display significant resentment of authority.
- Management places undue pressure on the auditors, particularly through the fee structure or the imposition of unreasonable deadlines.
- The client's profitability is inadequate or inconsistent relative to its industry.
- The client is confronted with adverse legal circumstances.
- Management exhibits undue concern with the need to maintain or improve the image/reputation of the entity.
- There are adverse conditions in the client's industry or external environment.
- Accounting personnel exhibit inexperience or laxity in performing their duties.
- The client entered into one or a few specific transactions that have a material effect on the financial statements.
- Client management is inexperienced.
- The client is in a period of rapid growth.
- This is a new client with no prior audit history or insufficient information from the predecessor auditor.
- The client is subject to significant contractual commitments.
- The client's operating results are highly sensitive to economic factors (inflation, interest rates, unemployment, etc.).
- The client recently entered into a significant number of acquisition transactions.[40]

Internal compliance teams Management may set up internal compliance teams to assist in promoting compliance with procedures. These teams do not relieve it of its responsibilities, since management must still be prepared to make executive decisions, even where based on recommendations made by internal auditors. The teams may be used to investigate frauds and irregularities and should have a level of independence so that they may work objectively. They may be applied to investigating minor frauds. Managers are responsible for resolving frauds and they resource this through the control team.

Personnel section Personnel may be seen as an independent function that may be used to formally communicate between the alleged perpetrator/s and management and ensure that personnel polices are being adhered to. This is relevant where management is investigating and taking action against the parties involved. Personnel have a dual role of advising management on their actions and ensuring that the rights of the employee are protected. Personnel disciplinary procedures must be observed by management.

Employees All employees should understand the fraud policy and know how to report suspicions of fraud. The Public Interest Disclosure Act 1998 offers some protection for workers who disclose information to a manager or his/her employer will be protected if the whistle-blower has a

> reasonable suspicion that the malpractice has occurred, is occurring or is likely to occur and can make a protected disclosure (which includes reporting a criminal offence) in good faith where:
>
> - the whistleblower reasonably believed he would be victimised,
> - he raised the matter internally or with a prescribed regulator,
> - reasonable believed a cover-up was likely and there was no prescribed regulator; or he had already raised the matter internally or with the prescribed regulator.

Returning to the IIA.UK&Ireland's Fraud Position Statement which contained a view on whistle-blowing:

> Internal audit may well have a responsibility to investigate allegations from whistleblowers although an external firm may be used as the contact point with the whistleblower to preserve their anonymity. It is good practice for larger organisations to have publicized systems for reporting fraud. If the investigation shows evidence of criminal fraud then the internal auditor must discuss the issue within the organisation but must also ensure that the issue is taken to the police.[41]

Others The ICAEW's audit faculty set up the fraud advisory panel in 1998 and went on to agree on three working parties to:

1. Gather intelligence and assess facts and information on fraud: where it is taking place; how much there is and establish reasons why there is poor reporting of fraud.
2. Establish methods of prevention; provide advice on fraud prevention and detection and how methods of training could be improved; make people more aware of the information needed by organisations and people at risk.
3. Consider the present offences of fraud; look at the effectiveness of existing investigation and prosecution methods and improve the speed of conviction as a deterrent to fraud.[42]

Investigating Fraud

When employee fraud or irregularity comes to the attention of the auditor there are a number of alternative courses of action. It is essential that each course is carefully weighed and the most appropriate action selected, based on the circumstances and the strength of evidence so far secured. These options should be kept under review:

Call the police This will be necessary where there is strong evidence of a fraud. The policy should be that the police are informed at the earliest opportunity. For more complicated concealed crimes, the police would expect the organization to have done some basic background work beforehand.

Commence a management enquiry This may involve a manager or management team being assigned to formally enquire into the circumstances of the case. This represents a responsible approach by management that acknowledges the importance of resolving frauds at once, say by interviewing all staff working in the area in question. It can spoil an investigation where those responsible are alerted and so are able to cover their tracks. If management, through lack of experience, do not cover all eventualities, then records could go missing, potential witnesses may be pressured and the investigation thwarted.

Commence an audit investigation The matter may be referred to internal audit for formal investigation. It may be kept confidential while a suitable strategy is formulated. An issue that is increasingly relevant is securing data held on PCs. If a suspect is alerted the files may be irretrievably wiped clean or destroyed.

Commence a joint management/internal audit investigation This is normally the best approach since it combines audit expertise with management's local knowledge in a suitable strategy. It also recognizes that management is responsible for investigating frauds.

Interview the officer in question There are times when this is the simplest option. It is possible to spend weeks investigating a matter, which, when presented to the culprit, he/she admits to straight away. Some fraudsters seek attention and want to be caught. It also allows simple explanations to be presented before the investigation has gone too far, for example, a case of mistaken identity or someone using another's computer access ID and password. The problem here is that, if little work has been done on the investigation, suspects may cover their tracks before any real evidence has been secured.

Suspend the suspect Where the evidence is strong and there is a real risk that losses may ensue if action is not taken straight away, then the suspect may be suspended. There needs to be a clear case and the decision should be reasonable and in line with the organization's disciplinary policy. The main difficulty is that while suspension does not imply guilt, an assumption of guilt tends to be made by others. Suspension means that evidence cannot be tampered with. It also makes a stronger case for dismissal at a later disciplinary hearing where one may be arguing that the person's presence at work can no longer be tolerated. But it will stop audit catching the person as the fraud is being perpetrated. Another disadvantage is that it may make it difficult to quickly convene an interview with the suspect who may resign before a case has been built up.

Instruct disciplinary proceedings We may wish to move straight into a formal disciplinary hearing based on the facts that are available. This is possible where we find that an employee has been convicted for fraud at court and this affects his/her position at work. It is better to carry out a full investigation beforehand and base the disciplinary hearing on the findings.

Check the system of internal control This is an important step and there are times when there is little that may be done. If a cheque has been stolen and fraudulently encashed then apart from advising the police there may not be much more that can be done. On the control side we might wish to issue a strict instruction that cheques issued by the organization should not be left on desks and should be locked away overnight.

Issue a formal instruction to staff This may sometimes be the most appropriate response. If it is clear that staff are overenthusiastic in, say, travel or overtime claims then it may be necessary to remind them that this is unacceptable and further distortion may constitute a disciplinary offence. We must be sure of the facts before making general comments and there are varying degrees of severity. Best practice suggests that employees should be told what constitutes a disciplinary offence and given sufficient warnings before a formal disciplinary hearing is applied.

Do nothing This depends on policy. It is possible to have a policy where anonymous phone calls making allegations where the person refuses to be seen (in confidence) are not followed up. This must be justified and arises where there are resource constraints and excessive levels of unfounded allegations.

The above options should be considered with care as soon as information is received on possible fraud and irregularity. A process of assessing the circumstances and selecting the right response should be established so that a sound decision may be made. Each of these options should be reconsidered periodically as an investigation progresses. It is possible to establish a formal policy whereby internal audit is informed immediately of all frauds, actual or alleged. Some argue that there is no one way to investigate a fraud since each one varies depending on the circumstances. This does not preclude us from developing principles for the investigation of fraud. One framework is shown in Figure 7.16.

Main Considerations

During a fraud investigation, consider the following:

1. **Planning the investigation.** The adopted strategy will have to be carefully selected, taking on board all relevant factors.
2. **Surveillance.** The use of this technique should be considered.
3. **Resources required.** The need to reassign resources will be high on the agenda. The IIA.UK&Ireland's Fraud Position Statement suggests several questions for the internal auditor to consider before becoming involved in fraud investigation:
   - Does internal audit have the necessary investigative skills?
   - Does internal audit have the necessary knowledge of the law?
   - When is the right time to involve the police?
   - Should internal audit be involved in this type of work and if so to what extent?

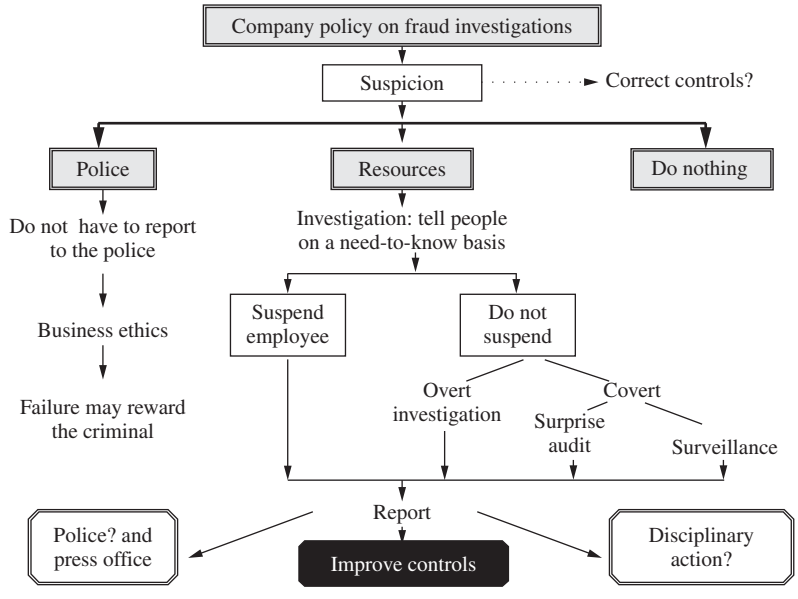


FIGURE 7.16 A process for investigating frauds.

4. **Recovering any lost funds.** At the outset of the investigation, identifying the extent of losses should be a major concern. This will affect the way that the ensuing work is carried out so that a confirmed 'schedule of losses' may be documented at the conclusion of the investigation.
5. **Legal status of the allegation.** Is it theft or simply breach of procedure? The police may be able to have an input on this matter. We have already suggested that a simple breach of procedure may turn out to be a major fraud.
6. **The level of evidence that has to be secured.** This will depend on the materiality of the fraud and the degree of difficulty in securing the available evidence.
7. **Limiting access to required documents.** It may be necessary to take immediate steps to protect files, documents and computerized records that contain evidence of the fraud. Where there is a clear suspect then this may be the best course of action.
8. **Management's role and the way that it will support the investigation.** This will vary depending on organizational policies. Where management shows no interest at all, then the fraud will be very difficult to penetrate. Where management is overenthusiastic then mistakes may occur, and a sensible middle ground needs to be achieved.
9. **The need to refrain from unfounded accusations.** Shooting from the hip is unacceptable. Even if we are sure who perpetrated the fraud, the case will rest on the evidence that supports our views and this can only be gathered through a careful process of investigation.
10. **Police involvement and advice.** Having a key contact at the local police station is very useful and this may be the first place for advice when the allegations first come to light.
11. **Staff interviews.** It may be necessary to meet with staff from the area in question as soon as possible. This may provide good leads to the culprit who may, unknown to the auditor, be one of the interviewees. It also has a deterrent effect as staff see that the problem is being taken seriously by management.

12. **The need for tight confidentiality.** One of the biggest questions that needs to be addressed is who to see. It is as well to keep the enquiries one step removed from the area of the fraud and work with a more senior level of management. Much information can be secured from sources that are accessed centrally, and it is here that the auditor's right of access becomes very useful. This also means that people outside the investigation team need not be alerted to the fact that the investigation is taking place.
13. **Surprise audit.** This technique may be used where there is a history of audit carrying out unannounced checks at organizational locations. Where this is possible, much inside information may be secured as well as checks made on relevant records without alerting the suspect(s).
14. **Recovery.** It may be possible to seek a restitution order to recover losses from the fraud. The judge should be advised of this during the hearing and may make a ruling if the defendant is found guilty.

Auditing To Spot Fraud, From Start To End

By Dan Swanson, Compliance Week Columnist

The Sarbanes-Oxley Act was enacted to help fight corporate fraud. Public companies have spent untold millions to comply and hired compliance and ethics officers ostensibly to ensure that the law is adhered to. Yet, somehow, at the end of the day, fraud is still here. However comprehensive your code of ethics may be, and however many policies you have, realize this one truth: Your organization could be the next one to hit the headlines. Simply saying, ''We strive for the highest ethical standards in our business,'' and passing that off as your ''tone at the top'' will never deter a morally challenged insider from ripping you off. Insider fraud is always a threat, and a company must always police against it. Once you understand that, it's just a matter of a modest investment of financial and human resources to implement and enforce policies and procedures with teeth.

Establishing A Robust Anti-Fraud Program

Some companies have significantly lower levels of misappropriation of assets and are less susceptible to fraudulent financial reporting than others. Why? Because they aggressively take steps to prevent and detect fraud. At these exemplary companies, management is responsible for designing and implementing systems and procedures for the prevention and detection of fraud – and, along with the board of directors, for ensuring a culture and environment that promotes honesty and ethical behavior.

Fraud can range from minor staff theft to misappropriation of assets and fraudulent financial reporting. It also can include embezzlement, identity theft, vendor fraud, conspiracy, and theft of proprietary information. Material financial-statement fraud also can wreak havoc on an organization's market value, reputation, and ability to achieve its strategic objectives.

The risk of fraud can be reduced through a combination of prevention, deterrence, and detection measures. Organizations need to adopt tough anti-fraud policies, strong internal controls, accountability on the part of all managers, training of employees in fraud awareness, liaison with law enforcement, and other ''brass tacks'' measures. Consider putting on the management committee's monthly agenda a standing discussion of what the organization is doing to reduce the occurrence of

fraud, and schedule a formal internal audit of the organization's anti-fraud program in 2007.

Evaluate Anti-Fraud Controls Regularly

Establishing an anti-fraud program is one thing, but there is nothing worse than having a policy that nobody follows. Identifying and measuring fraud risk is one of the first steps in implementing a robust anti-fraud program. Certain fraud risks also can be reduced by making improvements to the organization's policies, procedures, or processes, and fraud-risk assessments and fraud-risk management efforts contribute to the improvement effort.

Periodically conducting an internal audit of the anti-fraud program is very productive as an independent and objective assessment of current policies and practices. To do this, first conduct the fraud-risk assessment; then identify the key fraud controls and any control gaps; and finally test the effectiveness of the controls. Continuous monitoring by management and continuous auditing by the auditors are also very effective in tackling fraud directly. Many organizations are establishing continuous monitoring and continuous auditing efforts for their critical transactions and information systems; you should, too.

Risk Of Management Override

Yet another fraud risk threatens to undermine all of these efforts that have been discussed thus far: management override. A company can have stellar procedures to block fraud, but they won't do much good if the top brass simply allows some improper transaction to circumvent those procedures. Consider having the internal audit department independently review the month- and year-end accounting activities for any unusual transactions, such as suspect journal entries or reversals. You also should consider having an open debate at the audit-committee meeting on what the committee and the company itself are doing to reduce the risk of management override.

An Appropriate Oversight Process

The audit committee should evaluate management's identification of fraud risks, implementation of antifraud measures, and creation of an appropriate ''tone at the top.'' Active oversight by the audit committee also will help reinforce management's commitment to creating zero tolerance for fraud. The audit committee plays a critical role in helping the board of directors fulfil its oversight responsibilities for financial reporting and other governance activities. To assess risks of things like forgery, credit-card fraud, conspiracy, computer sabotage, Internet-based fraud and so forth, the organization and the audit committee should consider obtaining the advice of specialists, using internal or contracted resources to compile detailed reports regarding vulnerabilities and recommend fraud exposure-reducing actions.

The audit committee also needs to beware of enterprise-threatening fraud risks. While management must cover the entire spectrum of fraud risks, the board needs

to be focused on the significant fraud risks and ensuring that an effective risk-management strategy and supporting processes have been implemented. Having an ongoing debate about what the oversight process should be is a good thing, and evaluation of its effectiveness is even better. The parties contributing to oversight efforts include the board, senior management, the internal auditors, the external auditors, and (on occasions) certified fraud examiners. Knowing who is responsible for what, and when to lean on their expertise, will ensure a winning team effort.

Creating An Ethical Culture

The company is responsible for creating a culture of honesty and strong ethics and for communicating clearly the acceptable behavior and expectations of each employee. Directors and officers of the organization set the tone at the top for ethical behavior within the organization. Employees should be given the opportunity to obtain advice internally before making decisions that could have significant legal or ethical implications. They also should be encouraged and given the ability to communicate about potential violations of the entity's code of conduct, anonymously if need be (such as via a confidential hotline service). The Open Compliance and Ethics Group's Hotline & Helpline guide provides a wealth of guidance for implementing this important fraud reduction measure. It has been proven that the ability for staff to safely report issues will reduce the incidence and impact of fraud.

We also need to make managers more accountable for their operations, that is, we should not be waiting for audits to make changes. Management is responsible for the organization's system of internal control, and the effectiveness of its operation, and I strongly encourage managers to evaluate their own results. (It's called operational monitoring and process improvement.)

Be Diligent

An open discussion among the key stakeholders, and ideally prior to any front page news, is always recommended. Setting clear expectations for everyone involved (regarding your anti-fraud efforts) is half the battle. Being diligent in your efforts is the other half. To truly fight fraud, we need a firm policy that must be enforced, and violators must be investigated and action taken. Fraud-risk management is here to stay – has your organization implemented an effective strategy for fraud prevention, detection, and response? At the end of the day, are you part of – the problem or part of the solution?

Reprinted from *Compliance Week*. This article was originally published in Compliance Week. Reproduced by permission of Compliance Week. All rights reserved.

The Investigative Process

Although every fraud investigation will be unique, it is, nonetheless, possible to devise certain key stages and standardized procedures that may be applied to each one. These may be summarized:

1. Allegation received A clear policy should be established. The allegation can come from a variety of sources that include:

- detective controls – for example, a bank reconciliation;
- anonymous information – by phone or letter;
- formal complaint – say, from a supplier;
- concerns expressed by a line manager about his/her staff;
- whistle-blowers 'hotline';
- head office – on activities at a branch – say, less cash accounted for;
- an audit – which has picked up an unexplained problem;
- colleagues or friends who hear an employee boasting about underhand activities;
- the police who indicate that an employee is implicated in fraudulent activities;
- pure accident.

One may place limited reliance on anonymous accusations where the informant refuses to give name and contact number. If allegations come from several reliable sources, their status is higher. Line managers' concerns over a member of staff may be given close attention and members of the public satisfied their concerns are being properly dealt with. Auditors may come across unexplained discrepancies. All allegations should be documented and full details, including action taken, kept in a confidential file. This is particularly relevant since claims that the problems were covered up may later accompany allegations. There are many sources of information on illegal activities including routine audits, conversations, observations, MIS, systems of internal check, letters and phone calls. It is essential that the policy allows all allegations of fraud to be filtered through to internal audit so that centralized records may be maintained. Allegations could be the result of a grudge and/or incorrect information. It is important that a procedure is in place to pick up on any allegations (perhaps a frauds hotline) and that there is a considered method by which they are dealt with. If this point is not handled properly, then it is likely that the line manager will simply confront the employee in question and ask for an explanation. This will either cause claims of victimization (where the employee is innocent) or impair the investigation (where the employee is guilty and seeks to conceal the crime). There may also be claims of a cover-up where the manager speaks to the employee and decides on no further action. Each of these positions is unacceptable.

2. Establish the basic facts before firm action is taken Interview the person supplying information at his/her convenience. This gives the auditor a good idea as to the validity of the allegations as well as providing necessary background information. Contact names should be taken and a full write-up of the allegation made. A personal profile may be drawn up where there are defined suspects and information such as payroll, pension records, personnel, creditors, income, electoral register and Companies House may be used. It is possible to establish a defined list of details that relate to a suspect who may be placed on a checklist. This will include description, age, address, car, grade, length of services, marital status and sick record, without alerting anyone to the investigation. The preliminary enquires should ask whether the allegation could be true and it is important to work out whether the allegation/problem is possible to substantiate. Before we launch into a full-scale investigation there are several key questions that must be answered:

- Does the alleged perpetrator exist?
- Do the allegations come from a reliable source?
- Have we got enough information to form the basis of an investigation?

- Are we sure that the allegations are not malicious?
- Can we get more information about the circumstances behind the allegation?
- Could the problems presented to us exist?
- Is there any history of this type of allegation/suspicion?
- Are there any documents that could support the allegation and are they available?
- Is this a real fraud or simply a minor breach of procedure?
- Are there any obvious explanations?
- Could the problem result from innocent error?
- Are any supporting records supplied by the informant?
- Are the allegations consistent with other developments that we are aware of?

We can add to this list, although the important point to note is that this vetting procedure should be carried out by experienced staff (if appropriate, internal auditors) and should be fully documented for later reference. We may care not to act on a vague allegation from a disgruntled ex-employee (or any anonymous person) where indicators suggest that it is unfounded. If this is the case, we must be able to justify this position at a later date. Likewise, if we embark on a major exercise, we must be able to prove it was necessary as a result of information received. The key rule is to 'open a file' and record decisions made at this stage of the enquiries.

3. Carry out further background research This includes securing all information available to the auditor without entering the area where the fraud is located. It involves reviewing previous audit files and documents that relate to the location. A brief fact sheet may be compiled setting out an organization chart and background details. An auditor cannot, without permission, search a person, car, personal bags or home address. However, it is normally possible to search the suspect's office desk and filing cabinets. Once we feel that we need to act on information received, it is necessary to do some background work. We need to isolate the area under review, the persons who may be implicated and the assets that may be at risk. We must decide where the fraud is contained and mark this as the 'affected area'. Special rules will apply to dealing with this designated area so that the investigation may proceed unimpaired. The following factors will assist this process:

- Identify the exact work area subject to the allegations.
- Isolate what goes on in this area including documentation and information that is received by the unit/branch/section.
- Establish the outputs in terms of documentation, returns, reports and services that come from the affected area.
- Establish the staff involved and isolate potential suspects.
- For each suspect, compile a profile including name, age, role, job title, length of service, sex, description, car, address, National Insurance number and so on.
- Define reporting lines and structures in the section.
- Try to secure inventory lists and a record of assets (say, computers held).

We may care to access all corporate information systems such as payroll, personnel, payments, ordering, stores, pensions and others, in pursuit of the required information. It is as well to have several key contacts in personnel and other corporate sections where we may make discreet enquires about the people in question.

4. The preliminary report This indicates whether the allegation may be true and should be investigated. An overall strategy should be defined. Management should be shown the report and

a meeting held to discuss the implications. This is important because if it is shown there is no foundation for the allegations, then time is saved by avoiding a full-scale investigation. Alternatively, it may be more efficient to send a memo to staff where wide-scale minor abuse is evident, such as high levels of private phone calls or private photocopying, as a form of amnesty, after which action will be taken against continuing offenders. This may be the best solution and save audit time. The preliminary report will address how best the problem should be tackled and by whom.

5. Investigation plan This plan should be derived from discussions with management and will indicate the approach, work required, resources and any contact with the police or other authorities. The preliminary report outlined above will be used to derive a plan of action and may set the tone for relevant meetings with senior managers. The plan should set in motion the agreed approach so that all parties to the matter have a clear role with timescales attached to each task. Domestic arrangements such as accommodation, travel and communications should also be part of the plan. Also, the work must be carried out in line with clear documentation standards that should cover areas such as:

- defacing documents by writing on or marking original documents;
- the chain of custody in terms of possession and how the evidence has been stored, retrieved and applied;
- rules on obtaining documents via voluntary consent, subpoenas, search warrants and so on;
- key documents filed in chronological order;
- forensic examination of documents looking for alterations, date, forged signatures, comparison to other documents, opened envelopes, faint writing, fold and tears, fingerprints and so on;
- the need for a secure room to hold documents.

6. Managerial support The level of managerial support will depend on the fraud and the level at which it is alleged to have occurred. It is best to link with the level of management twice removed from the allegations. This ensures the manager is outside the range of the fraud. A decision will be made on audit/management roles and whether it will be a joint investigation. The reporting mode will be defined and how frequently these reports will be made. It is advisable to draft brief reports and present them orally to management since time is a prime factor in most fraud investigations. These reports should be made at least once a week and more frequently for high-risk investigations that need urgent action. It is good practice to keep the CAE informed by providing copies of the reports. The golden rule is to speak to management at least two levels removed from the affected area. It is normal protocol also to involve the director, although top managers may have little contact with operational staff. Much will depend on the levels of employees implicated. Nonetheless, it is good practice to brief the directors and maybe chief executive where a major or sensitive fraud is alleged. Moreover, we may have already discussed the case with management in terms of providing advice on urgent action that needs to be taken to close loopholes in controls that allowed the fraud to occur in the first place.

7. Defining barriers Throughout the investigation, it is necessary to work out possible barriers to the investigation such as missing documents, sources of evidence, the culprit's presence, close associates of the culprit, the need for confidentiality and records being tampered with. Where any of the evidence is at risk, swift action must be taken. An organization can assist by making the intentional and unauthorized destruction/removal of documentation a disciplinary offence. Computerized information, particularly that which is held on a PC, can contain valuable evidence and is at risk. Consider the different types of evidence that may need to be gathered and the

extent to which they could be tampered with, including documents and witnesses. There are certain at-risk individuals that need to be dealt with carefully, including:

- young people
- blind or visually handicapped
- illiterate
- people under the influence of drugs or alcohol
- mentally ill or handicapped
- people who need an interpreter.

8. Initial strategy New information will come to light and the adopted strategy will alter as necessary. The idea will be to cover all angles and find the best way of securing relevant evidence. The options of suspension, interview, notifying the police and so on should be continually reviewed. Some investigations have a funnel approach where they start out with a broad base and narrow down the relevant issues as new facts come to light. The strategy changes to become increasingly focused on key areas. These will be where there are outstanding queries or inconsistencies that cannot be explained without implicating defined individuals. Meanwhile, occurrences that at first sight appear suspicious may be explained as the investigation gets going. The detailed discussions with the suitable tier of management will be based around formulating an investigation plan. Our own audit policies will mean that the CAE and audit managers would have been advised early on in the enquiries and it may be that the CAE has to approve any subsequent action plan that is jointly agreed on with management. There are several options that may be considered, including the following:

- Suspend the employee in question immediately.
- Call in the local police (we may have already gone to them for initial advice).
- Undertake covert enquiries without alerting anyone not party to the exercise.
- Send out a general reminder to staff where a low level abuse of facilities is occurring.
- Carry out an audit of the area in question – this is particularly useful where spot checks are part of the normal audit approach.
- Carry out surveillance – we need to establish rules for this type of activity.

9. Surveillance Surveillance involves observing the activities of defined individuals without their knowledge. Watching, looking and gathering evidence does not generally breach privacy standards and is a useful way of securing information in a fraud investigation. It is sensitive and must be handled with care. One approach is to formulate a formal policy based on the premise that it should only be used when absolutely necessary. Some argue surveillance should only be carried out by experts. Simple undercover operations can yield results particularly where this is the only way of obtaining proof of a fraud. To carry out surveillance:

- **Plan the operation carefully.** Start with a clear objective based on the nature of the investigation. Surveillance is time consuming and resource intensive. It may be policy that senior management is informed and that an audit manager authorizes it and briefs the CAE beforehand.
- **Do a trial run.** One auditor will check the area for feasibility before resources are allocated. This provides information on the location, description, timing and useful tips for the full operation. A detailed map of the area should be constructed and copied to the team. The auditor assigned to the trial run must be experienced and look out for significant factors and interpret them.

- **Prepare by deciding resources and approach.** A briefing session with those taking part is a useful way to plan the work. A brief file may be made up for all team members with a report on the case, relevant personal descriptions, photographs, a map, specific instructions and blank surveillance records. Observation may be fixed point (static) or mobile and may involve tailing cars (or people). A motorbike is useful for some types of mobile observation although cars are much more comfortable in bad weather. Cameras, videos, dictaphones, watches, mobile phones and mobile phone links may be used. These should be signed for and batteries checked. On the move, it is difficult to buy fresh films, petrol or batteries. At least two people should be allocated to each team. There are practical arrangements such as the supply of sandwiches and drinks as well as the possibility of spending a long time on the job outside office hours. A home base should be designated that vehicles/auditors will return to when the suspect falls out of the frame. A mobile phone link should be arranged and one senior auditor should coordinate the activities ideally from a static point.
- **Action should be anticipated and authorized activity distinguished from the unauthorized.** Permission may be sought when using buildings for observation. Ensure vehicles are carefully positioned. It is a breach of privacy to follow someone into their house or garden. It is best to call the local police in the area under surveillance to let them know what is going on. Information from a surveillance exercise may not make sense until all the observations are put together.
- **If confronted during a surveillance, initially try to deny it while avoiding a conflict situation.** Avoid declaring the real reason unless the threat of injury is apparent. Keep the exercise secret on a need-to-know basis. There are tailored excuses that may be rehearsed for being in an area. This can range from carrying out market research through to waiting for a late partner. One cover is a couple who stand around for hours making small talk. On one occasion, a couple who appeared to be in a series of long embraces recorded fraudulent activities using a camcorder. Useful aids to the exercise include newspapers (held the right way up), a football or running in a jogging suit. Dictaphones may be used to record detail where a notepad would look out of place. Great care must be taken and the auditor should withdraw immediately if there is any chance of being spotted by the suspect.
- **Always carry an ID card** and take notes contemporaneously on a formal surveillance record. It is possible to write up formal notes after the event as long as this is done as soon as practicable and the rough notes are retained. The clothes worn should be chosen to suit the occasion. Anything out of the ordinary will arouse suspicion although there is no point in wearing a boiler suit to merge in with workers if strangers who appear on site are challenged.
- **Simple matters may be resolved through surveillance** such as the movements and whereabouts of an individual throughout a defined period. It is more difficult to determine why a person goes to a particular place or what the significance is for more complicated frauds. Simple breaches of procedure covering overtime, sick leave, work attendance and locations visited during the day are easier to prove. A court appearance will mean cross-examination of surveillance and other evidence. The auditor should only record what was seen and not make guesses or assumptions. If the exercise results in nothing of significance then this is a finding in itself and not a cause for embarrassment.

10. The full investigation Most of the investigation will involve obtaining confirmatory evidence in whatever form it is available. This may include reviewing documents, interviews, photographs, surveillance, analysis and/or tracing transactions. It is here that the real art of applying auditing techniques comes to the fore. We must seek to prove guilt by carefully compiling relevant evidence, although we should be careful not to be seen as acting as an *agent provocateur*. The

resource issue must be resolved, and this will alter as the investigation takes shape and changes direction. It will be linked to sensitivity and overall impact on the organization. Once we have agreed on an appropriate course of action, we need to consider the detailed plans. However, before we can arrive at this position, we need to decide on respective roles. The various options are as follows:

1. Management investigation with advice from internal audit (perhaps in the form of regular meetings or advice over the phone whenever required). This is useful where the fraud is mixed with general concerns over conduct, attendance, performance and other managerial issues.
2. Audit investigation where we take over the project. This is useful where senior managers are implicated, the fraud is large and covers many parts of the organization or where it is a covert exercise relying on access to many different information systems (and perhaps surveillance).
3. Joint investigation where management and audit form a team.
4. Joint investigation where a personnel officer (representing management) works with the audit team.
5. Police enquiry (or a joint internal audit, management and police enquiry).
6. Management board of enquiry where the investigation goes public and there are many witnesses who are asked to present information to the enquiry panel. Audit may act as advisors and carry out small exercises that are then fed into the panel in report format.

The format of the investigation will dictate the way it is structured and undertaken. In essence we take the view that a fraud cannot be said to have occurred unless we are able to present evidence that substantiates it. As such, the plan will be aimed at securing the requisite evidence in the most convenient and reliable manner possible. This may consist of:

- interviewing witnesses;
- analysing documentation;
- securing reports that tend to support the allegations;
- computation of financial losses;
- securing evidence of breach of procedure by comparing what happened with the approved procedure;
- observing activities and recording the results;
- reperforming calculations and reconciliation;
- securing evidence from independent sources that corroborate or conflict with other available evidence, perhaps to find out whether a cheque was received by a supplier listed on the payments database.
- assessing whether a document is forged, altered or subject to a forged signature.

Much of the above is about interviewing witnesses and extracting relevant documentation. One point that should have been discussed at the outset is the objective of the investigation. Although this will be to prove that the fraud has occurred, it may also be used to bring a prosecution in a court of law. In addition, it may be used to present internal disciplinary charges to a specially convened panel.

11. Ongoing review and discussions with management As the investigation progresses, its shape and form will alter as new information comes to light and all parties to the work become more familiar with the activities under review. It is important that there is an ongoing review with management (where audit are carrying out the investigation) and the plan is adjusted to take on

board new information. If the case has been handed over to the police, again we need to be kept up to date with enquiries as progress is made. This is particularly important where arrests are being planned. We would hope to have formed a close working relationship with the local police so that, what would otherwise be confidential information, may be freely discussed. One important consideration is how far to go back in the investigation. Where the fraud involves false claims (say on time sheets or overtime or expenses) over the years, we need to agree on a cut-off point so as not to have an open-ended enquiry.

12. Interviews A key component of most fraud investigations is the interview process. Here most questions can be addressed by simply asking the right people. Interviews may be held with:

- informants
- key witnesses
- line managers
- persons who may be useful to the enquires
- suspects.

Each has a different purpose and will follow a different format. The most important interviews will be with witnesses, who should be asked to provide a formal witness statement, and the suspect(s), who may be asked to sign a formal interview record. Witnesses will write down in their own words what they saw and heard, as relating to the issues in hand, and be prepared to present this evidence in court and/or at an internal disciplinary hearing. They may cross-reference their comments to various exhibits that will be attached to their statement and which were shown to them at the time the statement was taken. Suspects, on the other hand, will be asked to provide an explanation to evidence that points to them as perpetrators of the fraud in question. They should be cautioned in the appropriate format, which in the UK is as follows:

> You do not have to say anything. But it may harm your defence if you do not mention something which you may later rely on in court. Anything you do say may be given in evidence.

This retains the right of silence, but at the same time allows the prosecution to comment on any alibis that are produced at a later date. In addition, the Police and Criminal Evidence Act lays down certain rules for interviewing suspects in terms of allowing the interview record to be submitted to a court of law. In summary, these allow a right of silence and disallow practices that would constitute intimidation or duress. Most investigators now recognize that the suspect interview is not about extracting a confession. It is about presenting the evidence in front of the suspect to secure an explanation. If none is forthcoming, then we would seek to progress the investigation to prosecution stage. We may encourage a full disclosure, but this is a decision for the suspect (having been given the opportunity to seek advice from his/her lawyer). Note that we would expect most formal interviews with suspects to be carried out by police officers.

13. Interim reports Throughout the investigation, interim reports should be issued setting out findings to date, implications and further work recommended. It is for management to suspend staff, instruct the police, search desks and confiscate books and records, and the internal auditor should act in an advisory capacity. All major decisions should be made by management under advice from internal audit. These reports will represent a formal record of the progress of the

investigation and will be used in conjunction with the minutes of meetings held with management. They provide an account of decisions made through to conclusion. In terms of the organization's position, we will need a report that details the results of the investigation and the recommended course of action. It may call for the matter to be referred to the police, if this has not already happened. It may seek the suspension of the suspect concerned (again, if this has not already happened). It may suggest disciplinary action, if this is appropriate. The important point is that since internal audit is an advisory function, it is right and proper that action is taken by the corporate body of the organization. The audit report will therefore go to the corporate decision-making body for review and action, in line with the various recommendations. Top management should not be encouraged to wash their hands of frauds, simply because internal audit have undertaken the detailed groundwork. This is a key point in that it should mean that management present the case to the police, or represent the organization at court. It also means that management instruct disciplinary action against the person in question.

14. The final report This covers the necessary action that should be taken and may treat the activity as an internal matter or seek referral to the police. The report should address any immediate action on control weaknesses and may recommend a full systems review once the fraud has been dealt with. The recommendations should be sensitive to the welfare of the organization, and if staff have to be interviewed, this should be done through management in a carefully planned manner with a minimum of disturbance to the services provided by the affected area. When reporting, it may be practice to name individuals implicated or use a coding system with detachable keys that are kept confidential. All reports should be clearly marked confidential. The number of copies should be restricted and it is best to present them on a need-to-know basis. The report is not about giving an opinion of the guilt of the person, it is only to report the results of the investigation. The report may go on to state that there is sufficient evidence to support a case against a named suspect but it should not take a view on whether this person is guilty. Meanwhile, the information contained in the report is classified as confidential.

15. Criminal prosecutions and internal disciplinaries There tend to be two main results from fraud investigations. One is a referral to the police who will place a case before the Crown Prosecution Service with a view to bringing criminal proceedings against the parties in question. The other is that internal disciplinaries will be held against any employee where evidence points to his/her guilt in connection with the fraud. The first occurrence requires a prosecution where the court will determine whether the defendant is guilty 'beyond reasonable doubt', based on the evidence presented to it (and assuming the defendant pleads innocent). The second scenario requires the organization to bring charges of gross misconduct in front of a panel supported by evidence relating to these charges. The panel will judge on the less severe test of 'balance of probability' whether there has been a breach of internal discipline and then agree on a suitable remedy, which may result in dismissal. These two events can be initiated at the same time, since one is considering criminal charges, whereas the other is simply reviewing breach of internal procedure. The first is about the laws of the land, while the other relates to the mutual trust that underpins a contract of employment. It is essential that these two concepts are not confused.

16. Internal disciplinary action Employee fraud should be dealt with under the internal disciplinary procedure as gross misconduct, which is a dismissible offence. Internal action is not dependent on any ongoing criminal prosecution and should be taken at the earliest possible opportunity. The objective will be to permanently remove the employee from the workplace due to a breakdown in trust. If an employee appeals against an internal disciplinary hearing and

has exhausted the internal grievance procedure, he/she can take his/her case to the employment tribunal for unfair dismissal. This is why it is important to carry out the disciplinary procedure properly, that is, in line with the set procedure and, above all, in a reasonable manner. An alternative for the employee is to take the claim for unfair dismissal and go for independent arbitration (by ACAS). This much less formal approach involves the following procedure:

- Introduction
- Each side states its case
- Questions from arbitrator
- Parties summarize their cases
- Adjournment
- Arbitrator announces decision at a later date.

Even where a criminal case falls through, the employer can still defend a dismissal resulting from the internal procedure, which operates on the less demanding balance of probabilities (rather than beyond all reasonable doubt) – the test whether the employer genuinely believed on reasonable grounds that the applicant was guilty of the offence in question. In terms of taking internal action against an employee, there are certain principles that should be followed:

- Investigate and gather the facts carefully and compile the supporting evidence.
- Be specific about the charges and let the employee know what the complaint is about.
- Use counselling, training and support for less serious problems that demonstrate a learning curve – employee fraud is unlikely to fall into this category as it will tend to be a gross misconduct.
- Interview the employee and give him/her a chance to state his/her case. The employee should have a right to be accompanied by a trade union representative or colleague during any proceedings against him/her.
- Introduce the evidence and explain where it came from and give the employee a chance to explain and clarify matters.
- Determine the need to carry out further enquiries when given new information by the employee.
- Convene an independent disciplinary hearing where both sides of the case are heard and witnesses are examined and cross-examined before the panel adjourn to decide the case.
- Make clear the decision to both sides.
- Where the employee stays silent because there is an ongoing court case, then if evidence is sufficiently strong to require no explanation, the employer can go ahead with disciplinary action. The employee can only get an injunction to stop internal discipline where there would be a miscarriage of justice if it went ahead, which is quite rare. It is best to make the internal case about breach of procedure rather than use the terms 'fraud' or 'theft', which is what the criminal courts will be considering.
- Make full records of the hearing and provide copies to both sides if required.
- Provide an appeals mechanism where the employee is not satisfied that he/she has had a fair hearing.
- An employee on remand has not committed an offence that has been proved, so the internal case will have to be investigated. Where he/she has been given custodial sentence for an offence not related to his/her work, there may be grounds for dismissal, especially if it makes the person unsuitable for the type of work performed or results in frustration of contract. Where an employee conceals a conviction that is not spent, he/she may be dismissed having forfeited the employer's trust.

- The employer may give reference to a prospective new employer that the employee was facing unresolved disciplinary procedure so long as it is neutral, factual and probably fairly brief.
- The case may end up in an employment tribunal, an independent judicial body comprising a legally qualified person as chairperson and two other members; one is drawn from a panel of employer members, while the other is drawn from a panel of employee members. In certain circumstances, a tribunal chairperson may sit without lay members.

17. Final completed report We will complete the procedure by insisting that a final report is prepared on the fraud and action taken. This part is often missed as an employee is dismissed and the police take over the case. The confidential audit report may look like the one in Figure 7.17.

Executive summary

1. Introduction

Allegation and initial response

2. Investigation

Work carried out and detailed testing performed
A list of people interviewed will also be set out

3. Detailed findings

Detailed findings including suspects and evidence obtained

4. Conclusions and recommendations

Action required in terms of police involvement and disciplinaries
A list of disciplinary charges should be set out if possible
A whole section would cover controls and required improvements
(as well as any urgent changes that should have already been implemented)

Appendices

Schedule of losses – and details of recovery
Results of police case and disiplinaries
Any press releases and newspaper reports

FIGURE 7.17 Fraud investigation audit report – format.

Documentation

Each fraud investigation must be recorded in a formal file that contains all the relevant documents that have been secured during the course of the investigation. There are a number of general attributes of good working papers that should be applied to these files:

1. **Clarity.** It is good practice to insist that files are legible and can be understood by all potential readers. Neat writing with clear headings that guide the reader through the papers is essential, particularly since the files may have to be read without assistance from the auditor who performed the work.
2. **Indexed.** Each item in the file should be referenced and noted in a main index at the front of the file. As such, it should be possible to go directly to a specific document with ease.
3. **Support the audit decisions/opinion.** The findings and decisions made in the resultant report by the auditor will each have to be fully supported by firm evidence. The entire

investigation will be driven by this factor in terms of securing evidence to refute or support the allegations in question. When compiling the working papers, the auditor, in turn, must recognize and cater for this factor.

4. **Defend conclusions.** This builds on the previous point. One feature of fraud investigations is that as they progress, one may need to exclude defined individuals from the enquiries. This is a material decision bearing in mind that the auditor may personally know some of the people implicated by the fraud. At all stages, the working papers should clearly indicate why major decisions were made by investigating staff and what evidence was available to support these decisions. This may become an important factor if, at a later stage, the defendant claims that he/she has been victimized by management, which is a defence that is commonly used.
5. **The use of pro formas.** These can provide short cuts to what may be a fairly bureaucratic process of collecting and filing evidence. Interviews, meetings, analysis of documents and many other exercises may be recorded in a standardized format via the use of pro formas and this should ensure a more efficient approach to an investigation.
6. **Cross-referenced.** It goes without saying that the working paper file must be properly cross-referenced. The ability to retrieve documents instantly gives a good impression besides being very efficient. The police authority will be more positive in their response to audit findings if the papers are obviously readily accessible. Inadequate cross-referencing, on the other hand, will lead to embarrassing gaps as the evidence is presented by the auditor to management and/or the police.
7. **Economically used.** The realities of resource utilization mean that an investigation cannot go on indefinitely and this is also the case for the accumulation of evidence. Rules must be applied in terms of securing material for the working paper files based on practicality and the available resources. Each item must therefore meet this criterion before it is entered into the files. A decision may have to be made on how far the auditor should go back when accumulating evidence of a fraud.
8. **Headed up.** The principle that each paper must be properly headed must be applied. The idea is that each item must be separately identifiable if it became separated from the main file. We should be able to tell which investigation the paper belongs to and who compiled it (along with the date).
9. **Clearly shows the impact on the investigation.** Every fraud investigation changes as it develops and as new information comes to light. Throughout this process, the auditor, in conjunction with management, will make decisions that will affect the form and direction of the investigation. This process should be evident from a study of the working papers and each new document should be set within a defined time frame. One approach is to prepare progress reports on a regular basis, which refer to the documents that have been obtained. It is possible to date, stamp and sign each document (via a label) as it is discovered by the auditor. Lastly, the auditor may draft a file note that indicates the significance of any new material that has been secured. This might alter the objectives of the investigation, the resources required and/or add or delete a suspect from the enquiries.
10. **Signed by the officer and the reviewer.** This tends to be a standard audit requirement in that the file indicates who has carried out the work and the role of audit management in reviewing it.
11. **Show the work carried out.** The way this requirement is met will vary. It may consist of a brief note setting out what has been done perhaps in terms of analysing expenditure in the area under review. At the other extreme, the auditor may construct a witness statement that describes in detail the steps taken to formulate a specific document. The status and reliability of the evidence may be affected by the absence of this detail. It will reduce the possibility

of any defence challenging the evidence in court or at an internal disciplinary hearing. It is frustrating for an audit manager to pick up a file that contains lists of figures scribbled down by the auditor with no indication of what they represent.

12. **Set out the objectives of the work.** Much of the material that forms the basis of a fraud investigation is derived from the use of extensive testing routines. In this respect, it is useful to have for each test a clear objective statement possibly signed by the audit manager, which sets out exactly the aim of the test and how the ensuing results may be applied to the investigation. In addition to forming a formal record for the file, this approach should provide for greater efficiency in the work carried out.
13. **Indicate which matters are outstanding.** For completeness, it is a good idea to indicate whether there are gaps in the work carried out. An example would be a strategy whereby all staff working in a particular unit are interviewed as potential witnesses to the fraud. Where one individual has not been available, this should be clear from an analysis of the relevant documentation. It will be difficult to explain months after the event why one person was left out, particularly if the auditor in question has left the organization. It may be that a certain exercise was planned but, for some reason, was no longer required. Again the working papers should contain a suitable note to this effect.
14. **Dated.** This rule should be strictly applied.
15. **Show any impact on the next stage of the investigation.** Bearing in mind that we would have planned an investigation perhaps based on a planning document that has been submitted to management for discussion and action, where the direction of the original plan changes as the investigation progresses, this needs to be recorded so that the working papers reflect the changing path of the investigation.
16. **Complete.** All relevant documents must end up on the definitive audit files, which means that this should be the only file (or set of files) that is maintained. It is bad practice to hold many files in the office with each one containing copies of some evidence without making it quite clear which is (are) the original and complete file(s).
17. **Set out in a neat and orderly fashion.** Sloppy work should never be accepted.
18. **Consistent.** If interviews are typed after the event then this should be applied to all cases where an interview has taken place. Post designations and terminology should coincide, which is particularly relevant where more than one auditor is working on the investigation.
19. **Simple.** A great criticism of some fraud investigations is that they can become extremely complicated. This can create major problems for all parties involved, apart from the defendant. The state of the working papers can add to this state of confusion or make the whole matter manageable. The rule here is to keep it simple by having clear objectives, good evidence and ensuring that too many issues are not dealt with at the same time.
20. **Required.** A document/working paper should be secured only if it is required. This point is related to the level of resources that are applied to an investigation as the main benefit of using senior auditors is their ability to apply greater discretion when building up a file of evidence. Junior staff tend to apply the policy of 'when in doubt, put it in'.
21. **Includes summaries.** There is little point in accumulating a vast store of documents on the basis that each of them have a link to the allegations, however vague. The investigative process requires one to sift through the available material and extract only that which is necessary to prove the issues at hand and this does rely on some skill and experience. This concept is assisted when summaries are used to isolate the key features of documents that have been filed. This technique should be used wherever possible. It is certainly not acceptable to file large reports and schedules without indicating which parts are material to the investigation.

22. **Reviewed.** As per normal audit practice, the working papers should be reviewed by an appropriate level of audit management. This review should also be documented.
23. **Shows the source of information/data.** This is vital, and all sources should be clearly quoted so that any schedules may be reproduced if necessary. The date is also relevant as information, particularly financial data, does change over time as accounts are updated by the system.
24. **Logically arranged.** The information may be arranged to coincide with the progress of the investigation and this will help take the reviewer through the various stages as a case is put together.

When securing and storing documents from a fraud investigation the following steps should be taken:

- Handle all documents with care and protect them by placing them in polythene pockets. Preserve fingerprints by using forceps.
- Label all documents carefully (i.e. the pocket) and note date, time and location. Where a person admits using or having an association with a document, record this, for example, a diary belongs to him/her.
- Do not write on the documents or attach any sticky labels.
- Do not attempt to reassemble documents by using adhesive.
- Make sure the original documents are retained.
- Secure all ribbons in typewriters/printers significant to the investigation. Take a sample from the typewriter after the ribbon is removed and replaced. Take samples from the complete keyboard, lower and upper case.
- Try to obtain samples of handwriting from all suspects. The sample should match what it is being compared with.

Acting as a Witnesses

When acting as a witness there are certain guidelines that should be observed by the auditor:

- **Make sure you are familiar with court procedure.** There is a separation of prosecutor and witnesses so that no undue pressure is applied. Rules cover contact with other witnesses during the course of giving evidence and court protocol guides the witness when in court. If these matters are not in the audit manual, advice should be provided by the organization's legal officer. Any person representing the organization should be briefed about court procedure before attending a hearing.
- **Refresh your memory by reading your statements.** An auditor may ask to refer to his/her notes when giving evidence.
- **Do not discuss your evidence** with other auditors who may also be called as witnesses, as the defence may argue that there has been fabrication.
- **Think before answering questions.** The golden rule is to be honest; if the witness cannot remember precisely what happened, then simply say so. If the statement is inaccurate, this should be admitted. If something is a matter of opinion, then say so. If a request is made by the prosecution (say, to see an audit report) and the auditor is unsure whether it should be entertained, it should be referred to the CAE.
- **It is not the witness's job to please anyone in court**, only to present evidence in a fair and open fashion.

- **Keep calm if the defence seeks to discredit your evidence.** It is the role of defence lawyers to influence the jury. A weak defence relies on spotting gaps in the evidence and if any level of doubt/error can be brought out, no matter how immaterial, this may be used to cast doubt on the rest of the evidence. The tactic is either to discredit the documents presented by the witness (e.g. by the auditor) or discredit the auditor. The defence may sum up the case by asking the jury whether they are convinced that the investigation was professional after suggesting not. Resilience is necessary where a witness can remain calm and composed and keep hold of the vital rule of thinking before answering while keeping to the truth, the whole truth and nothing but the truth.

Formulating a Fraud Investigation Procedure

We have developed an investigations procedure within the context of the fact that no two frauds are alike. A procedure is a formal document that sets standards for the way activities are carried out and specific tasks undertaken. Fraud investigation is much like any other business activity although there are two main features that should be noted. First, they tend to be sensitive with a high embarrassment factor, particularly, if the investigation goes wrong. Second, the fact that an investigation is required constitutes another source of potential embarrassment where controls have failed and management has allowed this problem to happen. We are faced more with a damage limitation exercise where the investigation seeks to find the culprit, solve the problem and allow management to get on with its real work. This is why good procedures are required in this area of work. However, procedures by themselves offer little help. There must be an efficient implementation process whereby these procedures are translated into action and results. A summary of the factors underpinning these procedures can be noted:

1. Let the procedures be based on a culture of fraud prevention. Here, management seek to prioritize good controls so as to avoid systems breaches. Much is derived from a risk-based approach where assets at risk are identified and steps taken to assess the extent to which they are protected in a proactive manner.
2. Ensure that the organization has established an anti-fraud policy that is built into contracts of employment, management's role, directors' priorities, and dealt with at induction training and ongoing training and development programmes. A formal disciplinary code of practice should make reference to the anti-fraud policy.
3. The fraud investigation procedure may also be supported by formal fraud detection exercises where project teams are set up to isolate any particular frauds that are deemed to be of concern. This can target sensitive areas such as payments systems, payroll claims, cashier and money transfers, pension funds, treasury management (loans and investments), employee references, computer security, purchasing and contracts, cheque dispatch systems and so on. Any allegation or suspicion of fraud can feed into the fraud investigation procedure in a dynamic fashion. A special phone number for reporting suspicions is one way to encourage action, so long as there are rules attached to its use.
4. Train key staff in the investigations procedure. This will include internal auditors, personnel officers and key managers. Note that we must be careful about publicizing all our detection and testing methods as this may encourage people to 'beat the system'. However, good training is one way to ensure investigators know how to action the procedure if required.
5. Make sure the police are aware of our procedures and contact names and numbers. It is good practice to establish a liaison mechanism to keep in touch with the local police (or specialist police fraud investigations units).

6. Make the chief executive responsible for the fraud investigations procedure with advice from the chief internal auditor. Where the CAE is the nominated fraud officer, there must be a clear recognition that the CEO is ultimately responsible for tackling fraud through delegation to the appropriate officers. As such, all final fraud reports should go to the CEO along with reports of allegations and action taken and summary reports on fraud and irregularity over each reporting period (say, quarterly). It is as well to involve the audit committee and management team in the summary reports, under confidential cover.
7. Adopt a formal policy of *'zero frauds'* where each time a problem arises, we ask what went wrong, and how this can be solved. This may encourage fundamental questions such as whether we are employing the right people (where we have a high incidence of reported fraud), and so begins the search for better systems starting with recruitment, selection, performance appraisal and career development.
8. Ensure that there are effective mechanisms installed that mean the investigations procedure is reviewed, kept up to date and properly applied across the organization.

When a chief executive is asked what he or she would do if a fraud came to light, the following response would be apposite:

- I have a formal anti-fraud policy.
- I have a nominated frauds officer (maybe the CAE).
- I have developed a comprehensive fraud investigations procedure.
- This procedure is supported by standardized documentation and various training workshops.
- Meanwhile, I have installed controls that seek to minimize the risk of fraud in my organization.

If the CEO cannot provide this response, there is an exposure that will make their life potentially uncomfortable. Meanwhile, the chief auditor should be providing advice to the CEO on this and related matters in line with the procedure that we have set out above.

Practical Points

All frauds are different and fixed rules cannot be applied to unpredictable circumstances. A disciplined approach is based on compiling sound evidence from reliable and confirmed sources with the resulting documents put together in a systematic fashion. The following are practical points to note:

1. The police prefer cases to be well presented with the evidence clearly compiled. This enables them to resource the investigation and assign to it a degree of importance. If a case is poorly put together with obvious gaps, this will make it more difficult for the police to deal with it in an efficient manner. The ideal position is reached where a good relationship has been built up over the years between internal audit and the local police. In dealing with cases, the police will have defined their requirements and a level of trust will exist where the auditor's work is deemed wholly reliable.
2. We should determine whether the enquiry is an internal disciplinary matter or a case for the police. It is good policy to refer all criminal cases to the police or at least seek their advice. On the other hand, the implications for the organization must be considered for all cases even those that are being dealt with by the police. It is important that a separate case is developed for use in an internal disciplinary hearing that does not depend on the results of the police case.

3. The police should be assigned a liaison officer, which may be an internal auditor who will be in contact with them throughout the investigation. Auditors may assist where, say, a whole group of staff has to be interviewed, since a heavy police presence may disturb the services that are being provided. In this respect, it may be advisable for audit to undertake these interviews and present the results to the police. Again, these and other issues should be discussed with the liaison officer.
4. When an allegation first comes to light, it is essential that the affected area is defined, since any initial covert enquiries will have to be performed outside this area. This is particularly true where through lack of evidence, it is necessary to allow the fraud to continue and capture current evidence. Surveillance is an example of securing concurrent evidence to support the allegations. Secrecy must be preserved and this point should be repeated to all involved at every opportunity. Sometimes, it is better to take a case away from management, and report only to a senior manager, so this element of secrecy may be maintained. An investigation will eventually become public knowledge.
5. Where an employee is being investigated by the police as a result of an internal investigation, it is still possible to discipline this person. The person can be interviewed and disciplined without waiting for the outcome of the police case as long as the charges relate to internal matters, for example, breach of procedure as opposed to a criminal act such as theft. It is difficult to see how a fraud could be perpetrated against an organization without an accompanying breach of procedure. It is the breach that should be dealt with and this matter should be addressed in the disciplinary code of practice and job descriptions. It is a good idea to interview a suspect before he/she is arrested by the police. This is because a defence lawyer may recommend that any employee arrested in respect of a criminal offence should not discuss the case with the employer. We may go further and suggest that a disciplinary hearing may be held in the absence of the employee, although it is better to hear a representation from the employee before the disciplinary panel make their decision.
6. When an employee is accused of stealing the organization's assets, it is important that the situation is quite clear. Theft requires an intention to permanently remove the goods and one defence is that items are held at home for later use at work. If there is no clear policy, the courts may find it difficult to give a guilty verdict. A formal document should spell out exactly what is entitled to be kept at home and what must not be removed. A formal inventory should be devised with signatures for each item removed. It should be possible to show in court that an officer had no right to hold defined objects or use them for unauthorized purposes. If the policy is slack, vague or not applied, then any subsequent investigation will be hindered.
7. The standard of evidence will be high since it will be scrutinized in detail at any later court hearing or internal disciplinary hearing. Defence will attempt to find fault with prosecution evidence, and any minor error may be used to call into doubt remaining evidence, however accurate. The standard defence is to engender doubt in a jury's mind. If junior auditors are being used, they must be given clear instructions. The audit manager may organize the case so that he/she will present an item of evidence even if it was compiled by a junior auditor. On no account should an inexperienced auditor be left to the mercy of the defence lawyer at court, where the audit work is unreliable, not reviewed and unchecked. Regular team briefings will promote a consistent approach. It is advisable to give junior staff a clear insight into the nature of the fraud enquiry before they undertake their work on the basis that a better understanding of the objectives will encourage better results.
8. It is best for management to present disciplinaries and represent the organization in court while the audit role may be reserved as that of principal witnesses. Management is responsible

for investigating fraud. Audit may act as advisors and compile evidence in support. Audit may become experts in presenting evidence to court as reliable witnesses, while management will stand up in court and explain its procedures and describe how they were breached. Management would also present the case to a disciplinary hearing for a formal consideration and decision, while auditors will attend as witnesses. It helps if the precise roles of each party have been properly defined at the outset.

9. Under the Data Protection Act 1984, non-disclosure does not apply where the information is needed to detect crime or apprehend or prosecute offenders. Internal audit should have access to all information and explanations necessary for the performance of their work and an appropriate audit warrant will be issued to reflect this. There is a view that the Data Protection Act is infringed where one embarks on a 'fishing expedition' with no clear suspects in mind. This might occur where one is seeking to compare two computer files as a general fraud detection exercise.
10. The Advance Disclosure of Evidence Act allows defence the right to look at evidence before it comes to trial. This has an impact on internal audit since it will cover the original documents that were used to arrive at the audit opinion. Defence may also view material that was never published in the audit report but may have been used in the investigation. This applies to audit working papers, primary documents and related documents. The defence will make requests through the relevant police officer who will then make necessary arrangements. The auditor should always take the name and address of the person visiting and be present when documents are examined. The defendant is not entitled to see the documents, only the lawyers. Where photocopies are requested, the auditor should note these requests and supply them at a later date with a covering letter and accompanying invoice set at a reasonable rate. It is essential that the organization publishes a suitable policy on the arrangements for complying with the legislation.
11. When conducting an investigation, always open a file and adhere to the in-house standards on the following:
    - Always use indexes in all files.
    - Place original documents in plastic wallets.
    - Use photocopies (with the words 'I certify that this is a true and fair copy taken this day'; signed and dated).
    - Use interview notes and photographs (marked with dates, times, places).
    - Ensure that all information is recorded and all documents kept secure. Particularly sensitive material may be held under lock and key in the audit safe.
    - Retain the original documents and give copies to third parties, including the police.

The Fraud Control Project

It is possible to carry out a special review of controls over computer abuse/fraud planned using an established model as shown in Figure 7.18.

We would look for suitable controls over assets and information at risk. These would be evaluated to discover whether they were adequate and applied in practice and steps recommended to address failings found as a result of the project. It is essential that the project team report to a high corporate level within the organization with decision-making powers that can be used to take action on recommendations. Much of the work will revolve around the IT security officer, although, if there is no such person, then this may well be the first major recommendation. Fraud is not a natural consequence of using computerized systems, although there are differing views on this issue. Research has been carried out but there are

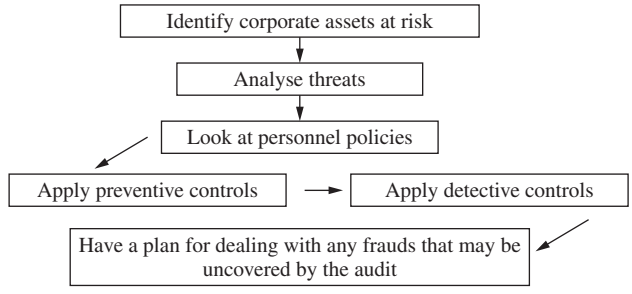


FIGURE 7.18 The fraud control project.

many organizations that protect their credibility by not reporting frauds and attempted frauds. Suitable controls have to be applied and audit's role remains the same in reviewing adequacy and effectiveness. The only supplementary issue is where internal audit makes a bid to perform a systems security role in the organization, although this is a matter that the chief internal auditor should consider and resolve. Fraud detection is about adopting a proactive approach to fraud by carrying out audit projects to seek out and eradicate specific frauds. This might be done in conjunction with the police who would provide advice and become involved where there is a clear case of criminal activities. Plan the audit with reference to:

1. the probability of fraud occurring within high-risk areas of the organization;
2. the staff required to resource such an important project including their qualifications, experience, skills and personal attributes, as the team should be hand-picked, based on a demanding job specification;
3. the extent, terms of reference and scope of the audit should be very carefully defined as this will have a major impact on the work done and direction of the audit. This factor should be kept under review since the scope may well change during the course of the work. This may also have a knock-on effect on the type of resources that are being used. One important feature may be the need to secure automated data profiling and interrogation skills for the project.

This work must be done in conjunction with management who remain responsible for dealing with fraud and irregularity.

Preventive Techniques

Larry Sawyer has published the now famous words on prevention, the better part of valour:

> How much better it is not to lose something than to have to go to the trouble of finding it after it is lost. How much better to prevent a person from stealing than to detect the theft, recover the loss, and jail the miscreant. How much better to remove temptation than to punish someone for having succumbed to the temptation. How much better for the internal auditor to be regarded as a constructive consultant than as a police officer or a prosecutor.[43]

The investigative process is reactive in that it is initiated as a result of an alleged fraud. Steps may be taken to guard against fraud. The importance of establishing sound control cannot be

overemphasized as most frauds could have been avoided with proper controls. We must also question an organization that fully resources the investigation of fraud while ignoring the control implications.

Unfortunately, those charged with performing these investigations may have little incentive to push the control angle if it will result in less work being available for them. Key controls include:

- Good recruitment procedures
- Supervision
- System of management accounts
- Up to date accounts
- Clear lines of authority
- Controlled profit margins
- Good staff discipline procedures
- Management trails
- Good controls over cash income
- Stores/equipment control
- Fraud hotline
- Well-trained and alert management
- Independent checks over work
- Regular staff meetings
- An employee code of conduct
- Good management information systems
- Publicized policy on fraud
- Good documentation
- Financial procedures
- Good communications
- Segregation of duties
- Anti-corruption measures
- Good all-round systems of control

Fraud Control Process

Most frauds are the result of weaknesses in systems of internal control. Management needs to establish an overall process for controlling fraud which includes:

Preventive controls These are the most important controls that seek to prevent frauds. We have noted that these cover policies on fraud, segregation of duties, internal audit reviews, good control environment, good overall systems and many of the other points dealt with earlier. These are the most efficient types of control in that they are aimed at averting any potential frauds before they occur. Effort directed at this stage of the business systems will pay great rewards even if this is negatively expressed as a lack of fraudulent activity. These controls provide assurances to management that they might concentrate on achieving business objectives without risking losses in those organizational assets that they are responsible for. Management, rather than being responsible for the assets, are more accurately described as being responsible for establishing adequate controls over these assets. This brings the concept of preventive controls to a higher profile, so allowing them to attract sufficient resources to be operationally successful.

Detective controls These controls are based on the need to pick up any irregularities as quickly as possible. These include techniques such as alert management, trend analysis, spot checks, supervision, exception reports and probity audits. The question to ask is, 'Can any frauds have slipped through our systems and if so how can they be picked up?' We must accept that not all potential problems/frauds can be dealt with via preventive controls and there will be occasions where irregularity is almost unavoidable. Detective controls are designed to pick up any systems offenders and are an essential ingredient in the control cycle.

Corrective controls Once a fraud has been picked up, it must be corrected. The corrective controls include defined fraud investigators, management action, insurance policies, systems

rectification and effective disciplinary action. There should be clear procedures covering the topic of restitution and insurance. As such, if a fraud is picked up, there needs to be an effective method of dealing with it in contrast to a hit-or-miss approach. Management must know who to contact, what will be done and how they can support this process of investigating the fraud. Figure 7.19 illustrates how some of the major controls may be arranged to form an effective system for controlling fraud and irregularity by addressing the need for:

- high-level corporate standards
- a nominated fraud investigation officer
- associated resources and budgets
- a fraud manual
- management information on frauds
- security over resources and IT system
- procedures for key areas such as purchasing
- a clear link into staff discipline.

Figure 7.19 provides an overview of fraud control.

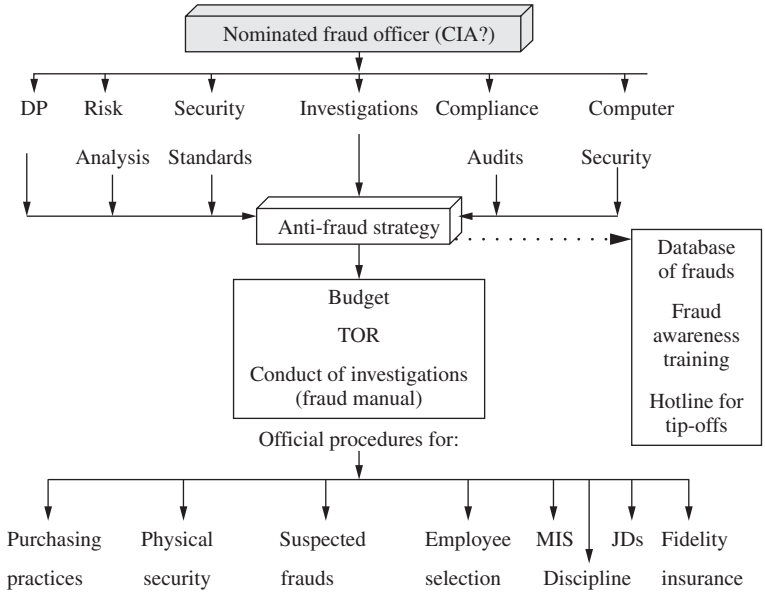


FIGURE 7.19 Overview of the fraud control process.

In this way, a whole system of controls can be devised across the organization to promote good security over organizational assets and resources. This is part of management's responsibilities that cannot be abrogated, although internal audit may assume a pivotal role. Fraud can be a very exciting topic and may be greatly stimulating for the auditor. There is much to learn, and many audit techniques, particularly relating to testing, may be applied to securing the underlying evidence that any case will be based on. There is, however, little developmental value in this role

and audit theory directs one towards operational reviews of systems of internal control as the true audit goal. Fraud takes a high level of resources and much planned audit work may fall to one side. A consultancy role, advising managers on how they might solve their frauds may be an efficient working relationship and this will have to be negotiated with the audit committee. If planned audit work is seen as a secondary issue, then the risk assessment process that identified these projects for the audit plan is obviously not working and should be reviewed. Systems weaknesses that allow frauds to occur should, however, be programmed into the audit plans and appropriate systems of preventive controls properly established. On no account should responsibility for guarding against and resolving fraud and irregularity be taken away from management. Neil Cowan has described internal audit's role in 'Company-wide fraud offensive':

> Internal auditing can play an important role in the fraud-prevention process. As specialists in control and risk, auditors are particularly well-qualified to educate employees throughout the organisation on how to minimise instances of fraud and to increase awareness. Auditors can help to ensure that fraud prevention is on everyone's agenda and foster a cooperative approach to the problem. Empowering employees at all levels to take an active role in fraud prevention can help to ensure that everyone contributes to this team effort.[44]

This is not straightforward and there are warnings that can be issued.

> Four dangers face the internal auditor who uncovers a fraud:
>
> 1. The audit may be defined by alerting the perpetrator early.
> 2. Auditors can become subject to civil litigation, such as libel, slander or false arrest.
> 3. Career damage may occur. This is particularly true when the fraud occurs at a high level within the organization.
> 4. The fourth danger that an internal auditor faces is that of violence.[45]

But at the same time, there are the challenges. Mark R. Kolman has described what it is like to live dangerously:

> In some instances, for example, auditors may be strongly discouraged from pursuing a fraud investigation because senior management does not want certain information publicized, or because they are financially and politically connected to the parties involved in the fraudulent activity. Audit management may overlook poor business decisions because they are intimidated by members of senior management and fear retribution. In some environments, where corruption is more pervasive, auditors steer clear of certain areas literally to avoid placing themselves in harm's way. This is, unfortunately, the reality of our profession, but it is also one of the reasons that we often fail to live up to the objective and independent commitment the profession promises to provide. To preserve our professional integrity and ensure the health of our organizations, auditors must be willing to take a stand on ethical behavior. Are you willing to live dangerously?[46]

The IIA make it clear in Attribute Standard 1210.A2 that the internal auditor should have sufficient knowledge to identify the indicators of fraud but is not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud. Moreover, the most effective way of managing the risk of fraud is to build this factor into risk assessment workshops that are performed by teams across the organization and so ensure prevention is part of the overall business risk management strategy.

Establishing Accountability for Your Antifraud Efforts

By Dan Swanson, Compliance Week Columnist

Some companies have far lower levels of misappropriation of assets and fraudulent financial reporting than others. Why? Because they aggressively take steps to prevent and detect fraud, end of story. At these exemplary companies, management takes seriously its ethical responsibilities for designing and implementing systems, procedures, and controls to catch fraud – and, along with the board of directors, for promoting a culture and corporate environment that demands honesty and ethical behavior. How does your company stack up? Well, run through this checklist:

- Does your organization have a strong fraud oversight process at both the board and management levels?
- Does your organization have robust and effective antifraud policies, procedures and controls?
- Does management regularly evaluate fraud risks and antifraud controls?
- Have the risks of management override and conflicts of interest been independently reviewed within the last 12 months?
- Would you say your workforce has a strong ethical culture?
- Does your company have a corporate policy that encourages whistleblowers to come forward? And do those would be whistleblowers actually believe it?

If you answered ''yes'' to all of the above questions, great. You're well on your way to a strong antifraud effort. Now answer three more questions that will help you get ahead of the crowd:

- What are the board's and management's roles regarding fraud?
- What should the internal audit team's role be regarding fraud?
- How can the organization best help the external auditor meet its responsibilities for evaluating fraud risks?

To answer that last question properly, you need clear answers to two questions immediately preceding it. Specifically: The board is responsible for defining and approving the organization's overall strategic direction and system of internal control, as well as for setting the tone at the top (overall corporate governance). Management operates the business within the guidelines set by the board, periodically reporting on performance and progress toward key strategies and objectives. Management also monitors operations. That includes regular assessments of the effectiveness of the overall system of internal control against the requirements set by the board, as well as the company's own ethical values and beliefs.

As mentioned earlier, the board is accountable for ensuring an effective system of internal control is established to fight fraud; management is responsible for how that system is designed and enforced to fight fraud. Once you have that clear – and actually done – the internal audit department can also contribute to those antifraud efforts.

Audit's Job: Helping Fraud Prevention Efforts

Today there is the belief that auditors are looking for – as well as investigating and stopping – frauds. After all, aren't auditors the last line of defense in identifying

crooked management? Well, no. The truth is that nobody can catch all fraud, and the internal audit department should address the misperception that this is internal auditing's purpose. Everyone in the company has a role in fraud prevention and detection, and the primary responsibility lies with all members of management (and by that, I mean managers at every level of the company).

An effective internal audit function improves the company's ethical culture and control environment, both overtly through its audit work and in a more general sense by promoting good practices. Internal audits of antifraud activities provide valuable feedback to management and the board on where they can improve overall performance, which contributes in the long term to more effective fraud risk management efforts. It can also be a deterrent when employees know that the internal audit department employs persons with fraud detection knowledge, skills, and tools.

Internal audit should design and plan audits specifically to detect fraud, which directly strengthens the organization's internal control system. The internal audit plan should be driven by an audit risk assessment (that is, the risk that an audit might miss something); likewise, efforts against fraud should be driven by a fraud risk assessment, because the greater the organization's exposure to fraud, the more antifraud audit effort must be allocated. And you must conduct fraud risk assessments thoughtfully, since it helps nobody to have your workforce believing the internal audit team distrusts everybody.

Audit work should include evaluating the organization's efforts in fraud prevention, fraud detection, and fraud investigation. If ''detective'' procedures are not in place, frauds that are discovered will require more investigative effort and result in greater loss. Over the long term, fraud prevention and deterrence efforts have the most impact on reducing fraud, so this should be a top management priority and be regularly evaluated by internal audit.

Always remember that auditing provides only a reasonable level of assurance; auditors cannot, and will not, provide an insurance policy against every possible fraud. But because of their objectivity and integrity, internal auditors are able to reinforce an organization's antifraud effort by investigating reports of possible fraudulent behavior. In fact, more and more corporate internal audit departments include trained forensic accountants.

There are numerous fraud audit techniques today, and more should be incorporated into audit departments. Some simple examples of forensic exercises include: correlating employee names, addresses and other contact details against the supplier database to help identify suspect transactions; examining expenses claims closely; following up religiously on seemingly insignificant discrepancies in control totals; using data mining and computer audit techniques in general to craft and answer cunning questions; and always being aware of the possibility of collusion, deception, and fraud. Some useful antifraud management practices include:

1. Identifying potential indicators of fraud for your industry, company, or activities within your organization;
2. Communicating with experienced people to learn ideas about how frauds may be committed and best detected;
3. Devising and routinely running tests to look for fraud indicators and data anomalies;

4. Performing ad-hoc inquiries as needed to dig into the source data underlying fraud indicators and data anomalies; and perform or include as part of control self-assessment sessions.
5. Implementing continuous auditing.

Norman Marks, a chief internal audit executive at Business Objects and old hand at internal auditing at large companies, recommends that internal audit periodically assess:

- The adequacy of the control environment, including: the adequacy of the code of conduct and processes to ensure it is understood, the adequacy of the whistleblower and investigation processes, and the staffing and organization of those responsible for the prevention and detection of fraud. Internal audit should go beyond traditional techniques such as interviewing or issuing a questionnaire only to senior management; a direct and more useful technique is to ask the workforce via surveys, interviews, and focus groups.
- Management's risk assessment as it relates to fraud and theft, including: whether the process is systematic and most conceivable fraud schemes identified, fraud risks adequately assessed, and appropriate strategies implemented.
- Management's monitoring activities, including: whether actual losses are monitored and compared to risk tolerances, and actual losses monitored to identify areas of concern, potential failing of controls, and opportunities for improvement.

There will always be limits to an organization's antifraud capabilities. Your sample sizes can only be so large. Your budget is only so big. Fraudsters, meanwhile, are cunning people who work hard to conceal their activities and exploit weaknesses in controls.

Organizations Must Be Ever Diligent

An open discussion about the possibility of fraud (of serious fraud), and the necessary responses, is always vital. Ideally, your company should have that discussion before a serious fraud incident rather than afterward. If you want confirmation of that, look at Societe Generale reeling from the multibillion-dollar fraud committed by one person. Now is not the best time for SG to ask how such a thing could happen.

Setting clear expectations and defining everyone's responsibilities regarding your antifraud efforts is half the battle. Being diligent in your efforts is the other half. To fight fraud, we need a firm policy, it must be enforced, and violators must be investigated and appropriate actions taken. Management must understand that it has the responsibility to design and implement antifraud activities, including the monitoring of the results. Internal auditors should also search for fraudulent activities and contribute to the organization's ''no tolerance'' attitude toward fraud.

Once your own house is in order, also consider the potential fraud risks relating to your key business relationships. Whistleblowing by suppliers, partners, or customers is one of the most common ways of discovering fraudulent activities, and it cuts both ways. If a worker at one of your business partner companies wanted to report fraud

at your company, would that person have the means (and the encouragement) to do so? What if one of your employees discovered fraud happening at one of your partners? How would you deal with it?

Reprinted from *Compliance Week*. This article was originally published in Compliance Week. Reproduced by permission of Compliance Week. All rights reserved.

7.6 Information Systems Auditing

The IIA Performance Standard 2120.A1 states that the internal audit activity must evaluate risk exposures relating to the organization's governance, operations and information systems regarding the:

- reliability and integrity of financial and operational information;
- effectiveness and efficiency of operations;
- safeguarding of assets;
- compliance with laws, regulations and contracts.

while standard 2110.A2 makes it clear that

> The internal audit activity must assess whether the information technology governance of the organization sustains and supports the organization's strategies and objectives.

The IS auditor has a particular interest in the first item – the reliability and integrity of financial and operational information. Meanwhile, Practice Advisory 2130.A1-22 goes on to say as follows:

1. The failure to protect personal information with appropriate controls can have significant consequences for an organization. The failure could damage the reputation of individuals and/or the organization, and expose an organization to risks that include legal liability and diminished consumer and/or employee trust.
2. Privacy definitions vary widely depending upon the culture, political environment and legislative framework of the countries in which the organization operates. Risks associated with the privacy of information encompass personal privacy (physical and psychological); privacy of space (freedom from surveillance); privacy of communication (freedom from monitoring); and privacy of information (collection, use and disclosure of personal information by others). Personal information generally refers to information associated with a specific individual, or that has identifying characteristics that, when combined with other information, can then be associated with a specific individual. It can include any factual or subjective information – recorded or not – in any form of media. Personal information could include:
   - Name, address, identification numbers, family relationships;
   - Employee files, evaluations, comments, social status, or disciplinary actions;
   - Credit records, income, financial status, or
   - Medical status.
3. Effective control over the protection of personal information is an essential component of the governance, risk management, and control processes of an organization. The board is ultimately accountable for identifying the principal risks to the organization and implementing appropriate control processes to mitigate those risks. This includes establishing the necessary privacy framework for the organization and monitoring its implementation.

4. The internal audit activity can contribute to good governance and risk management by assessing the adequacy of management's identification of risks related to its privacy objectives and the adequacy of the controls established to mitigate those risks to an acceptable level. The internal auditor is well positioned to evaluate the privacy framework in their organization and identify the significant risks, as well as the appropriate recommendations for mitigation.

The internal audit activity identifies the types and appropriateness of information gathered by the organization that is deemed personal or private, the collection methodology used, and whether the organization's use of that information is in accordance with its intended use and applicable legislation.

Given the highly technical and legal nature of privacy issues, the internal audit activity needs appropriate knowledge and competence to conduct an assessment of the risks and controls of the organization's privacy framework.

In conducting such an evaluation of the management of the organization's privacy framework, the internal auditor:

- Considers the laws, regulations, and policies relating to privacy in the jurisdictions where the organization operates;
- Liaisons with in-house legal counsel to determine the exact nature of laws, regulations and other standards and practices applicable to the organization and the country/countries in which it operates;
- Liaisons with information technology specialists to determine that information security and data protection controls are in place and regularly reviewed and assessed for appropriateness;
- Considers the level or maturity of the organization's privacy practices; depending upon the level, the internal auditor may have differing roles. The auditor may facilitate the development and implementation of the privacy program, evaluate management's privacy risk assessment to determine the needs and risk exposures of the organization or provide assurance on the effectiveness of the privacy policies, practices and controls across the organization. If the internal auditor assumes any responsibility for developing and implementing a privacy program, the internal auditor's independence will be impaired.

Complicated information systems have major implications for the internal auditor. Auditing around the computer described the traditional approach to auditing computer-based systems. This meant adjusting the usual audit approach without applying additional expertise in computerized applications. Another term was the black box approach where the computer was seen as a foreign object to be ignored by the auditor. Nowadays, the audit response must take on board strategic changes in automation, otherwise audit is left behind. One response is to define an audit role that specializes in reviewing computerized information systems as 'information systems (IS) audit' and this is the subject of this section. There are differing views of IS audit with many believing that all audit sections should employ specialist auditors. Others feel there is no such animal as the IS auditor since tackling computerized applications is part of everyday audit life. Computer audit tends to be known as IS auditing, as we move from the idea of auditing computers to the view that we are helping to turn raw data into a reliable and secure platform for decision making as set out in Figure 7.20.

Information Systems Risk

The risk of poor information systems and unreliable security and backup arrangements leads to possible fraud, error, non-compliance with data protection rules, customer dissatisfaction and

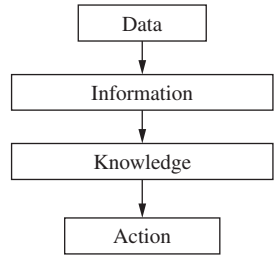


FIGURE 7.20 Control information.

security breaches. Poor information systems can undermine an organization, where the entire reputation of the organization may be at stake. The IIA.UK&Ireland's Information Technology Briefing Note Three covered Internet Security (A Guide for Internal Auditors) and suggests a number of IS risk areas

Theft of proprietary information	Sabotage of data or networks
Eavesdropping	System penetration
Abuse of Internet access	Fraud
Denial of service	Spoofing
Viruses	

Meanwhile, a 2002 Computer Crime and Security Survey highlighted the growing problems of cybercrime:

> Computer Crime continues to hit organizations hard, yet most don't report information security breaches to law enforcement, a recent U.S. survey reports. Ninety percent of the 503 U.S. organizations that responded have detected computer security breaches in the past 12 months and 80 percent acknowledged suffering financial losses, according to the seventh annual 'Computer Crime and Security Survey' conducted by the U.S. Federal Bureau of Investigation and the Computer Security Institute (CSI). The 44 percent of organizations that disclosed the amount of financial damage they suffered reported losses of $455.8 million. Last year, 85 percent of respondents detected computer crimes, and organizations lost $377.8 million, according to the 2001 survey.[47]

How to Weigh IT Investment Decisions

By Dan Swanson, Compliance Week Columnist

Corporate management has always been told to invest wisely in IT. The board has always been told to ensure management invests wisely in IT. It's a truism everyone states all the time. Too frequently, however, IT investment decisions by management and the board have relied on, and even deferred to, managers of the IT function. That results in what I call the Black Hole approach to IT investment: Throw enough money into technology, and we'll get something of value in the end. Corporations can, and must, do better than that. IT is now central to every core business process, and core business processes are central to sound governance. Can more formal, cohesive decisions about IT investment therefore improve your corporate governance? I think so – but those decisions must be directed by the business managers, not the technology managers. The board and executive management must also constantly

monitor the company's significant IT expenditures and participate in all major IT investment decisions.

For years business has encouraged IT to focus on delivering business priorities. At the same time, IT has tried to be an integral part of business planning and align IT efforts and investments with business priorities. At the end of the day, effective IT investment really does require the ongoing and engaged involvement of all key participants. Decisions regarding IT investment in your compliance and other governance initiatives should be driven by management and the board; IT managers should only be providing advice and counsel.

Where does one start? The company's strategic planning effort should be the first place to look; that is, the board and senior management need to define their strategic direction, key priorities, objectives, and draw up a ''roadmap'' to get there. After all, if the company hasn't defined where it wants to go, all the IT investment in the world won't help it get there.

Apply that same discipline when contemplating governance and compliance. What goals does the business want to achieve? How can IT help it meet them? Answer those questions, and then start mapping out your various compliance and governance efforts and the core IT needs; that is your blueprint to guide your IT investment decisions.

The IT Department's Role

IT planning efforts must be integrated with a company's business plans. And since business plans change and priorities evolve, the IT function needs an investment management process so it can continually refine its own priorities as the overall business priorities evolve. IT also needs to acquaint the business with what is currently possible, and at what price. IT needs to explain the consequences and opportunities the business direction imposes on technology.

If not actively involved in the strategic planning processes, IT management at a minimum needs to understand the company's strategic directions and plans in detail. Simply reading strategy papers will not suffice, since important elements of business strategy often aren't written down. Think about who really develops strategy at the company, and cultivate a conversation with those people. Engaging with the company's strategic development and investment management processes is one of the most important roles of the CIO and other senior IT executives. Particularly for compliance and governance efforts, IT needs to be aware of best practices in the industry – a topic most IT managers don't know all that well, frankly – and bring forward innovative solutions to tackle problems such as increased regulatory reporting requirements, endless refinements to the compliance and ethics program's information needs, and so on.

Finally, by matching IT investment decisions to the company's long-term business plans, IT can go beyond the chronic problem of having too few resources for the current budget cycle. With a longer perspective in mind, the inevitable tactical quick-fix imperatives can be balanced against genuine strategic IT initiatives. Prioritizing and coordinating IT investments needs this broader view. IT also needs to deliver its own assessments of opportunities and threats and work with the company on how to mitigate (or take advantage) of them. Key takeaways:

- The CIO and other senior IT executives should actively participate in the organization's business planning.
- The organization's leadership should be involved in IT strategic planning and investment management activities.
- The board should ask management to describe how business planning and IT planning are being integrated and encourage frequent and ongoing dialogue between board members, the management team, and IT leadership.

The Internal Auditor's Role

Although achieving and maintaining IT-business alignment is really a management issue, the internal audit department can help. Internal audit evaluation of an organization's strategic planning efforts, including how IT supports the business priorities, can provide valuable feedback to the board and senior management. An audit of IT investment processes should determine whether:

- significant business priorities are appropriately identified and assessed on an ongoing basis;
- changes to those priorities are monitored;
- significant investment management controls are operating effectively and consistently;
- risk-management techniques are in place and effective;
- management and staff have the processes in place to recognize and respond to new business opportunities as they arise; and
- IT-related investments are effectively and efficiently managed.

There are two distinct elements to most audits of IT investment management. First, the auditor evaluates the specification, design, and implementation of the IT investment management processes. Then the auditor examines how the IT investment management processes actually operate, including an assessment of the business priorities currently being addressed. And how would this improve IT investments in compliance and governance? By helping to ensure the organization is defining its business priorities and has an investment process that aligns IT expenditures to those priorities.

Four Critical Issues to Evaluate

Does management have a strategic IT plan in place that is updated regularly and supports the annual plans, budgets, and prioritization of the various IT efforts?

Ideally, an IT strategic plan would be developed and approved by the board, although the IT planning document may take many forms. It could be a separate IT plan, something combined with the organization's overall business plan, or a series of business case submissions over time.

An overall strategic planning process regarding IT investment and IT spending prioritization should exist. Always remember that business planning should drive the IT priorities and IT investment decisions; that's critical. Successful projects happen when business management retains control of the initiative and sets clear and balanced business requirements.

What level of investment in IT (and IT security) has occurred in the past two to three years? What is planned for the coming two to three years? Is there a reasonable level of expenditure, compared to the overall operating and capital budgets? While no specific level of investment in IT can be labelled ''appropriate,'' management should be able to explain the reasonableness of the IT and IT security expenditures in relation to the overall capital and operating budgets. The IT expenditure trend should be in line with the business and IT plans. A key board concern is always whether the company is spending too much or too little on IT and IT security.

Have the roles and responsibilities for IT management and oversight of IT investment been defined and assigned within the company? The responsibilities for the various IT activities within the organization related to IT management and IT investment should be defined and assigned to specific personnel. There should be a logical allocation of IT responsibilities within the organization.

Does management monitor IT's performance, as well as IT's capability to continue providing the services the company relies on? What are the major issues reported to senior management regarding IT and IT security? Is there a healthy debate at the board level regarding concerns raised by management or the board? If not, what could be done to improve the situation? This question also explores the operational monitoring that is performed by management regarding IT operations – and whether IT is outsourced or managed internally, it should be occurring.

Practices That Support Alignment

Key management practices driving more effective alignment, and consequently improving IT investment results, have been identified by the IT Process Institute. They include:

1. Identify opportunities to use emerging technology to meet business objectives.
2. Have an effective process and methodology for justifying and prioritizing IT investment decisions.
3. Develop and enforce enterprise infrastructure standards.
4. Have a project management office function to provide oversight to business prioritized IT projects.
5. Have a formal periodic process for the IT department to identify what is needed by the business.

Oversight of IT investment must be integrated into a company's ongoing strategic planning effort, to ensure IT efforts consistently contribute to the organization's priorities. Executive management should revisit how it defines IT investment priorities, and the board should encourage a review of current practices to identify key improvement priorities. With limited dollars available, investments in IT for compliance and governance improvement must be balanced with other competing priorities; involving all key stakeholders in that reconciliation will help move the organization forward. There should also be an organizational culture that encourages IT and the business to work together continually.

Reprinted from *Compliance Week*. This article was originally published in Compliance Week. Reproduced by permission of Compliance Week. All rights reserved.

The Role of the IS Auditor

The role of audit in computerized information systems is vital to the continuing welfare of the organization. The high cost of investing in IT in terms of set-up costs and its impact on achieving objectives results in an abundance of control implications. The biggest task may be to control this aspect of the organization and if audit is kept out of these issues, their role will be relegated to minor matters only. The IS auditor may review a system (Figure 7.21), for example, creditors, and must be able to bring into play important operational matters such as setting out terms of reference for the audit clearly:

- Start with the business objectives.
- Recognize that many controls are operational and interface with automated controls.
- Plan computer auditor's work with this in mind.

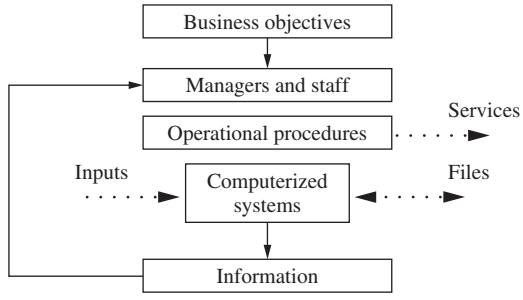


FIGURE 7.21 Business objectives and information systems.

The new-look internal auditor must recognize the link between the business activity and the computerized systems used to facilitate this process of setting and achieving business objectives. The IS auditor will concentrate on risks to the input, process and output aspects of the system (i.e. everything below operational procedures in Figure 7.21), while the operational auditor will pay more attention to the controls located in the upper section of our model. Both audit approaches must acknowledge each other in a supportive and communicative manner. Application controls have to be tested by the auditor in line with the requirement that all audit findings should be supported by suitable evidence. Auditing around the computer means relying on management to provide all the necessary testing information and schedules and this does not promote audit independence or enhance the audit knowledge of the systems under review. The auditor may incorporate a systems control review file within the software to extract interesting information. In addition, parallel simulation may be used to set up the auditor's own model of the programmes that are being run. Interrogation software may also be used to obtain suitable audit samples for analysis while test data may be used to test the correct functioning of the documented controls. Internal audit may use application audits to establish a level of credibility within the organization and among computer specialists. Lessons for the audit approach may be learnt and this might affect plans for developing audit expertise, software packages and review techniques. The auditor should ensure audit objectives are met and there are no 'no-go areas' where the auditor is locked out of the system. Computer skills will be required so that systems controls may be identified

and tested without undue reliance on the computer department. Applications audits follow the same principles as other system audits and have the same audit objectives. The main difference is the nature of information systems that are reviewed and the type of controls that management needs to implement. IIA standard 1210.A3 makes it clear that not all auditors will have specialist computing skills:

> Internal auditors must have sufficient knowledge of key information technology risks and controls and available technology-based audit techniques to perform their assigned work. However, not all internal auditors are expected to have the expertise of an internal auditor whose primary responsibility is information technology auditing.

There are several options for securing the necessary IS/IT skills for internal auditing:

- Use a consortium to provide the necessary skills.
- Use a small number of IS auditors (perhaps one computer expert) to assist the other auditors as they tackle computerized systems.
- Train general auditors in IS audit techniques.
- Rotate auditors between groups with one group specializing in computerized systems.
- Use consultants either to perform certain computer audit projects or to assist the general auditors.
- View computer audit as the audit of MIS and apply a wider base to computer audit projects covering managerial controls as well as computerized ones.

Selecting an appropriate option from the above will ensure that this aspect of audit work is properly covered. If this issue is ignored, the resulting credibility gap may lead to competitive disadvantage. All auditors should be able to review computerized applications and information systems may be a major component of an operation's system of internal controls. In addition to buying in IS audit skills, it is necessary to train and develop auditors involved in this aspect of audit work. All auditors should go through a continuous process of acquiring IS audit expertise so that they become competent auditors:

- Avoid isolating the IS audit staff from the rest of the audit department. As one guideline for success, one could measure the extent to which computer audit interacts with other auditors. An incompetent IS auditor is generally one who speaks in terms that no other auditor understands and attempts to create an air of mystique around the whole function.
- Encourage auditors to take professional auditing examinations since a computer auditor who does not understand the principles of auditing is a liability.
- Programming courses can be very useful.
- There are IS audit training courses available but these must relate to the day-to-day work being performed or little value will be obtained.
- IS auditors can train other auditors in computer audit techniques.
- One-off seminars and lectures may bring staff up to date with the academic research.
- IS audit workgroups, particularly where they specialize in relevant types of operating systems and networks, can impart knowledge across audit departments.
- Directed reading can keep auditors up to date with current developments in the fast-changing world of computing. Subscriptions to monthly and weekly computer journals should be established.

- Courses on advanced IS audit techniques can build on existing skills.
- All training must be linked to career development and the costs of this training must always be worth the defined resulting benefits to the audit service.

Well-planned training programmes, alongside field experience on relevant projects, lead to highly skilled IS auditors, although the better individuals are mobile and may leave at short notice. If an MIS approach is adopted the auditor may wish to trace information systems through to the decision makers who rely on the information. The IS auditor is best used advising other auditors on how to develop and apply a suitable level of computer expertise. As such, the chief auditor may decide to assign IS audit time to main operational audits so that input, processing, output, file controls and security issues are addressed and incorporated into the overall audit. The difficulty in interfacing computer-based controls with the whole system of controls is more a conceptual matter that will impact on the audit approach. One model calls for the IS auditor's work to be interfaced with general auditor's work and there is a growing support for the development of all-round auditors with the requisite skills who are concerned that:

- the information should be clear, complete, relevant, consistent, sufficient, useful and timely;
- information should be accurate and based on correct processing of data;
- information should be secured and distributed according to defined criteria;
- it should be produced economically;
- it should be effective in meeting the objectives that have been established in the first place;
- there should be a process of continual review and adjustment;
- someone should be responsible for the information and the above objectives.

Auditing Records Management

By Dan Swanson, Compliance Week Columnist

Auditing a records management program in many ways should follow the traditional program audit. To wit, review the program's goals and objectives; assess what has been implemented to achieve them; identify opportunities for improvement; evaluate program performance; and report your audit analysis and recommendations. In particular, however, records management includes maintaining your compliance records. Many companies have compliance policies but do not understand why this area is so important; that is, they do not monitor compliance and record the effectiveness of that compliance. Such sloppy recordkeeping can leave companies exposed. Waiting until a lawsuit strikes is not a good time to determine if your records management policy is being followed.

Engagement Planning

Defining the audit objectives is the first and one of the most critical steps in setting the audit direction. This step should include understanding the company policy, goals, and objectives for records management and understanding who owns the process, how compliance is monitored, and how best practices are determined. This step also defines the level of assurance the board and management will be provided. Internal audit teams should discuss that with management and the board, to understand just how much assurance they want. The audit should also review both paper records and electronic records, as each have different risk profiles, and you'll need to explore the assurances wanted for each. Some possible audit objectives include:

- Determine if the records management program is documented, in place, and appropriately resourced to meet the organization's needs.
- Determine if the program is in keeping with current good practice based on size and complexity of the organization.
- Determine whether any other audit objectives as needed by the board, a board committee, or management, are being met.

The nature of the organization affects the nature of the audit. A large multinational organization has different business issues and challenges than a small business. As such, the generic audit procedures provided below must be ''customized'' to fit the organization's environment and the assurance needs of the board, management, and other stakeholders.

The general steps in the internal audit process include:

- Define the scope, goals, and objectives of the evaluation.
- Define the organization's assurance needs.
- Identify the evaluation team and skills required.
- Develop the evaluation plan.
- Perform an evaluation of the design's adequacy.
- Perform an evaluation of operational effectiveness.
- Communicate evaluation results and ensure follow-up to address issues.

The planning phase defines the components of the audit project plan and includes developing the:

- Purpose of the audit
- Description of the program (i.e., the entity to be audited)
- Audit scope and scope exclusions
- Audit objectives and approach
- High-level audit schedule and detailed audit timeline
- Necessary skills and the internal audit team
- Other resources as required.

Engagement Testing

The audit itself can involve a wide range of tests. For example, look at the consistency and integration of records management among business units within the enterprise. Do they all follow the same policies? Do they all train compliance officers in the business units with the same goals and policies in mind? Do they all produce the same sort of measurable results?

Other avenues of testing might be to explore:

- The coordination between the central office and individual business units on records management.
- Confidentiality of the information handled by the records management staff.
- The use of emerging technologies and other best practices in meeting today's (or better yet, tomorrow's) records management needs. For example, new rules for

e-discovery in civil litigation impose tough new expectations that companies will be able to identify and procure relevant records in short order. Can you do that?
- Coordination between records management overseers and other departments that might need access to the company's whole realm of data, such as the legal department putting a ''hold'' request on certain e-mail messages relevant to a lawsuit.

The audit team should evaluate the records management efforts regarding its effect on organizational performance, scope and strategy, structure and resources, management of policies and training, and ongoing improvement efforts.

The auditor should ensure there is an up-to-date understanding of the records retention requirements of all localities where the auditor operates. For example, can documents be retained in electronic form? Special attention should be given to the approvals for destruction of documents. Special attention (perhaps very special attention, depending on your industry or company history) should also be given to the retention of documents that are or may be involved in litigation.

Engagement Reporting

Among the primary purposes of internal auditing is to provide the board and management with objective assessments about the design and operation of management practices, control systems, and information. To accomplish this objective, internal audit must effectively communicate audit conclusions and recommendations. Throughout the audit, the internal auditor should discuss findings and potential recommendations with management. This helps to ensure that the auditor has considered pertinent information when forming conclusions and provides an opportunity for the internal auditor and management to develop effective solutions for identified deficiencies.

At the end of the audit, this informal communication process is formalized through closing/exit meetings and written reports. The reporting phase of the audit project includes debriefing management, drafting the audit report, issuing initial and subsequent drafts, reviewing management action plans, preparing the summary report for the audit committee, and distributing the final audit report. Put another way, tell them what you did, what you found, and what management intends to do going forward. A records management program must meet the organization's needs and the growing regulatory requirements. Compliance requirements are becoming a greater driver and people are not investing to keep up with the risk. Auditing the program provides an opportunity to complete a comprehensive review of today's program and provide management with an analysis of the key opportunities for improvement. Management and auditors must survey emerging practices constantly, to ensure their organizations are adapting new and better practices regularly. For many industries as a whole, and for pieces of virtually all industries (such as the tax department), records retention and retrieval is a legal requirement; you want to ensure the organization is meeting these requirements. Finally, for most organizations, how and when you destroy records is vital. Think of Arthur Andersen, and remember: Record destruction should be a part of every records management audit.

Reprinted from *Compliance Week*. This article was originally published in Compliance Week. Reproduced by permission of Compliance Week. All rights reserved.

The IS auditor will ideally have some expertise in areas such as:

- systems development and projects;
- computerized applications such as payroll, payments, income, performance reporting and so on;
- information systems security standards;
- computer assisted audit techniques (CAATs);
- systems development and project management;
- disaster recovery and contingency planning;
- e-business and Internet design and security;
- overall information systems strategy;
- data protection and legal requirements;
- specialist technical areas such network management and database management systems.

Some of these areas are briefly covered below. One way of distinguishing the roles of general and IS auditors is by breaking down the audit universe as in Figure 7.22.

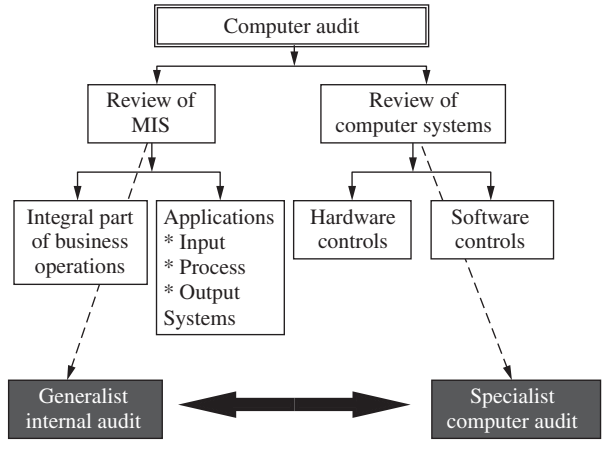


FIGURE 7.22 Analysing the computer audit approach.

Computerized systems affect the applied audit approach and there are many control features. General systems auditing can be used for any activity and depends on an understanding of the system being reviewed. As already mentioned, the IS audit role has moved towards the IS audit format and in one sense has moved closer to the general auditor's role as the two dimensions become increasingly blurred.

Auditing a Company's IT Strategies

By Dan Swanson, Compliance Week Columnist

Today's IT solutions are complex, and they are getting more challenging to implement all the time. One of the great questions for management at any company these days is simply whether all the investment in those systems is worth it. Internal auditing can play a critical role there, measuring and inspecting how the IT investment process – specifically, how IT investment is managed – works.

There are two distinct elements to most IT investment audits. They are the evaluation of:

(1) How that management process is ''scoped out,'' designed, and implemented; and
(2) How that management process then operates, including an assessment of the business priorities currently being addressed.

An audit of IT investment management should identify whether the various management processes involved are operating well and what the key opportunities for improvement would be. The audit should evaluate whether management has an effective investment prioritization process in place, including the ongoing identification of changes in business priorities and new business opportunities. IT investment management also involves the evaluation of performance of IT initiatives, and the audit should assess the performance monitoring completed by management.

In general, an audit of investment management should let internal auditors provide an opinion on process effectiveness, an assessment of the organization's efforts to align IT with business priorities, and assurance to the board and management that the organization is working on the right projects.

Ten Questions to Answer

Audits of any IT system, and especially audits of how IT investment is working, will have many questions. Exactly which ones you'll need to answer and include in your audit planning will depend on your company's specific circumstances, but I've listed 10 of the most important ones below.

1. Are the organization's planning activities appropriate to its needs? The planning process should support management's awareness of, and response to, new and emerging business opportunities. The scope and formality of planning needs to be in line with the organization's needs and complexity.
2. Has an effective IT investment management process been developed and implemented? Every company needs a process to decide which initiative gets funding. Every company should also consider a balanced investment in operational, tactical, and strategic IT areas. Of course, the level of funding in each category will vary widely depending on the business environment a company faces and the strategic direction it is taking. But all of those areas should at least be considered, even if the dollars devoted to any specific one is zero.
3. Is accountability well established, and acknowledged by those to be held accountable? Management and staff need to know what they are responsible for. When it comes to management of IT investment management, we want to ensure that IT investments support the company's business and business efforts. This requires an investment decision-making process that is clear and relatively transparent. Identify the people at your company who participate in that process, and make sure they understand the consequences when the decisions they make produce bad results.
4. Are there appropriate systems, policies, procedures, and guidelines relating to IT Investment management? Describing how things get done is always beneficial.

For something as important as, ''Are we working on the right projects?'' formal policies and procedures are worthwhile.

5. How successful is IT in meeting business needs? Assessing whether your company is effective overall is always challenging. Perhaps the best we can achieve is determining what the key opportunities for improvement are.
6. Do we need to increase the alignment of IT efforts and business efforts? If so, what else needs to be done? At the end of the day, a company and its IT department must do everything necessary to get a grip on the organization's IT investment priorities to ensure the company is focused on business priorities – rather than on IT systems.
7. Does management have a strategic IT plan that is updated regularly and supports the annual plans, budgets, and priorities of the various IT projects? Companies should define the long-term direction of their IT needs, and auditors should be able to see a rationalization of what the company's IT spending priorities are, and why. Ideally, an IT strategic plan would be developed and approved by the board, although the documentation may take many forms such as a separate IT plan combined with the organization's overall business plan, or a series of business case submissions over time. The auditor should look for a demonstration of an overall strategic planning process regarding IT investment and IT spending prioritization. Also remember that business planning should drive the IT priorities and IT investment decisions, which means both corporate management and IT management will need to be interviewed.
8. What level of investment in IT and IT security has occurred over the past two to three years, and what is planned for the next two to three years? In other words, are IT expenditures reasonable compared to the overall operating and capital budgets? While no specific level of investment in IT is deemed to be appropriate, the auditor should assess the reasonableness of the IT and security expenditures in relation to the overall capital and operating budgets. They should also review whether the expenditure trend line can be explained by the business and IT plans. Is there a process in place to manage the expenditures involved with IT and IT security?
9. Have performance indicators for the IT function and IT security been developed? Are those indicators periodically reported to the board? Auditors should know what major issues have been reported regarding IT and IT security. A healthy debate should exist at the board level when these issues are presented by management (and, yes, management should be presenting these issues to the board).
10. Does management monitor IT's performance, as well as its capability to continue providing the services upon which the organization relies? This question explores the monitoring of IT operations that management performs – and whether it is outsourced or managed internally, monitoring should be done. The formality of the monitoring can vary greatly, although outsourced arrangements probably need more monitoring, and so it should happen more frequently.

The bottom line is that management of IT investment must be integrated into the organization's ongoing strategic planning effort and ensure that IT efforts consistently contribute to the organization's priorities. Perhaps it's time executive management revisited how it defines IT investment priorities. An audit is a good place to start.

Reprinted from *Compliance Week*. This article was originally published in Compliance Week. Reproduced by permission of Compliance Week. All rights reserved.

IS Audit Planning

Taking the view that IS auditing is a separate function attached to internal auditing, there is a need to plan the audit coverage in an efficient manner. An IS Auditing Guideline suggests that risk assessment is used to plan the use of IS audit resources by considering the following:

- The integrity of IS management and IS management experience and knowledge;
- Changes in IS management.
- Pressures on IS management which may predispose them to conceal or misstate information (e.g. large business-critical project over-runs, and hacker activities).
- The nature of the organization's business and systems (e.g. plans for e-commerce, the complexity of the systems and the lack of integrated systems).
- Factors affecting the organization's industry as a whole (e.g. changes in technology, and IS staff availability).
- The level of third party influences on the control of the systems being audited.
- Findings from and date of previous audits.

At the detailed IS control level (controls over the acquisition, implementation, delivery and support of IS systems and services), the IS auditor should consider, to the level appropriate for the audit area in question:

- The findings from and date of previous audits in this area.
- The complexity of the systems involved.
- The level of manual intervention required.
- The susceptibility to loss or misappropriation of the assets controlled by the system.
- The likelihood of activity peaks at certain times in the audit period.
- Activities outside the day-to-day routine of IS processing.
- The integrity, experience and skills of the management and staff involved in applying the IS controls.[48]

The work of IS audit must be properly planned and managed. Unplanned work is difficult to control. Once the role has been defined and a policy on the interaction with general auditors is in place, formal plans may be published. Some work will be internal and provide a support to the audit function on individual projects, automation and CAATs. The way computer equipment is acquired, used and maintained is another issue on which direction must be provided and audit standards play a vital role. It is necessary to set out the audit field before assessing each individual component. A useful way of analysing the audit field is shown in Figure 7.23.

The main issues within an automated environment range from the three main components of computerization: applications, IT support and IT/IS standards. Risk analysis may be applied so that high profile sensitive areas may be targeted. IS audit work must be planned and audit management needs to define the audit approach, the type of work carried out and the areas that will be audited. An appropriate methodology will flow from the professional principles of auditing and the guidance provided to the audit function should be documented in the audit manual. The way IS audit is organized and staffed should be carefully planned since the computer department may set up artificial barriers. If audit mirrors this by setting up a mysterious free-floating group of technical auditors with higher status than the rest of audit, the same dysfunctional factors arise, which may make them a separate uncontrollable function. The trend now is executive information systems and local expertise at operational level, which also applies to internal audit as users of corporate information systems. If the IS auditors do not spend most of their time developing internal

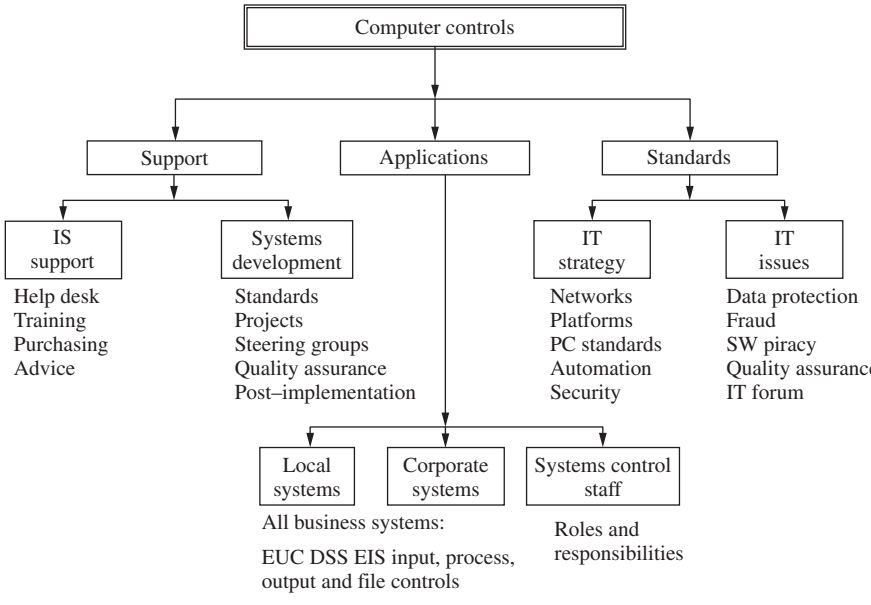


FIGURE 7.23 Components of computer auditing.

resources to get auditors inside complicated systems then there may be little scope for delivering a comprehensive and professional audit service. In terms of managing IS audit resources, note that:

- a cycle of audits may be planned to cover all of the main computerized applications;
- it will be necessary to set up a constructive liaison with the corporate IS managers;
- the difficulties in recruiting good quality IS auditors have already been mentioned;
- the depth of technical expertise should be defined in an appropriately worded job specification;
- the timing of IS audit work has to be planned as systems tend to take turns in securing a high profile as the organization's strategy alters;
- a budget for IS audit should include high-specification computer facilities along with notebooks, scanners, quality printers and so on, for use by auditors;
- the audit manager must carry out or arrange a technical review of the IS auditor's work. Work must be properly supervised;
- the work that IS audit performs on systems development may become part of the systems of internal control; as such, the role should be clearly defined at the outset;
- IS auditors may spend time supporting the audit function by developing CAATs and the way this is resourced has to be agreed via the audit plan;
- developing a comprehensive range of control matrices covering automated systems can aid control evaluation and this may well be an IS audit task.

IS auditors should be encouraged to become operational auditors and acquire a good understanding of managerial systems of internal control as well as the computer-based controls.

The Audit Role in Systems Development

The audit role in the organization is to:

- **Assure:** Assure management that systems development (SD) mechanisms work.
- **Alert:** Alert management where there are significant risks.
- **Advise:** Advise management on how these risks might be managed.
- **Act:** Act promptly to secure better management of risks.

This is the case even where we are involved in auditing systems under development. We have gone full circle in that the responsibility to establish suitable systems of internal control moved from audit to the computer staff, and is now seen to belong entirely to systems users. Users want good systems and will turn to all the available professional help in this struggle. This must include internal audit and we must meet these expectations in providing the professional support. Attention directed towards quality assurance arrangements over the adopted SD methodology may be the best way to use audit resources. Work on individual systems becomes part of the way audit tests the adequacy and effectiveness of the adopted corporate project methodology. Audit involvement in developing systems is called pre-event auditing by some, in that:

1. The auditor should ensure that the development process itself is sound.
2. The defined development process should also be seen to be applied in practice.
3. Adequate controls should be built into the new system at development stage.
4. The auditor should be prepared to give professional advice although if this is not based on firm evidence, then the opinion must be qualified accordingly.
5. The systems development should be consistent with the organization's corporate policies.
6. The required control evaluation should be carried out before the contract is signed.
7. The auditor should become involved in developing systems since independence cannot be guarded at all costs.

The idea behind pre-event auditing is to minimize the need for subsequent changes and the auditor must be prepared to provide practical advice. More recently, the involvement may fall under the consulting arm of internal auditing services to add value to the way new systems are built and brought online. Poor IS development can lead to many risks for an organization, including:

- substandard systems coming online;
- unauthorized changes to the system;
- systems that are inflexible and difficult to amend as circumstances change;
- business interruptions and general loss of client confidence resulting from system failures;
- a general loss of confidence among management and staff;
- fraud, another well-known danger;
- excessive costs indicating that investment in computer facilities has overshot budget and perhaps the whole computerization programme;
- violation of laws owing to poor systems particularly relating to data protection legislation.

Systems can easily fail where the specification is inadequate and as it runs over budget, senior managers start to distance themselves from the potential fallout. Normally, an organization tries to do too much too quickly and this can mean that many new systems coming online are faulty. The two main techniques for ensuring good systems come online are project management and SD standards. One way of viewing the value of an information system is to measure the extent to which it meets the four main criteria set out in Figure 7.24.

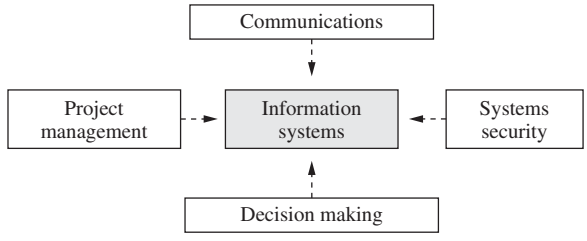


FIGURE 7.24 Effective information systems.

These four criteria should mean that the information system:

- is derived from sound project management;
- is based on the way people communicate within the organization;
- conforms with IS security policies and procedure;
- leads to effective decision making.

Systems' development is probably the most important aspect of any computerization programme ensuring the various criteria are acknowledged. The success with which an organization controls new and enhanced systems directly affects the success of resulting systems. The accepted definition of controls covers all those arrangements management establishes to ensure objectives are achieved efficiently. Audit resources directed at the SD process are well used. The new system has to meet competing needs as does the SD process. These different needs must be taken on board since all of these parties are users and their various expectations should be fully understood. Most new systems are enhancements or replacements where new software releases extend the existing system. Smaller more compact solutions tend to be based around PC-based systems. The IS auditor will look for the SD life cycle that is an established procedure for managing new systems (Figure 7.25).

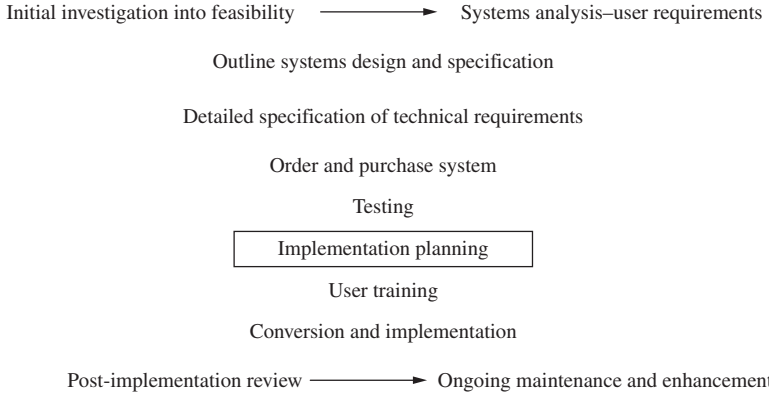


FIGURE 7.25 The systems development cycle (SDLC).

When the development encourages the early involvement of users it will have more chance of success, while the use of rapid applications design techniques (and purchased software packages)

will ensure that smaller systems get them in quickly. Meanwhile, good project management brings the whole initiative to fruition by seeking to reconcile the time, quality, cost and forces, and methods such as PRINCE 2 incorporate factors such as:

- project board;
- project manager (PM);
- the person leading on each stage of the project reporting to the overall PM;
- project assurance team;
- project initiation and plans (technical and resource plans);
- end-of-stage assessment;
- quality reviews;
- risk logs – risk and mitigation;
- controls – project initiation, end-stage assessments, mid-stage assessments, checkpoints, project closure;
- checkpoints – regular technical and management control points; checkpoint meetings conducted by the stage manager to measure achievement against plans to date;
- project stages – 1. project proposal, 2. project initiation, 3. project initiation meeting, 4. project planning, 5. managing and reporting progress (quality reviews), 6. end-stage process, 7. project closure.

The most damaging problem is a failure to interface the information, technology and operational implications of the new development. A one-dimensional view of the system as simply information and supporting technology will provide an inadequate view of the development. New or enhanced systems consist of three main business components as illustrated in Figure 7.26.

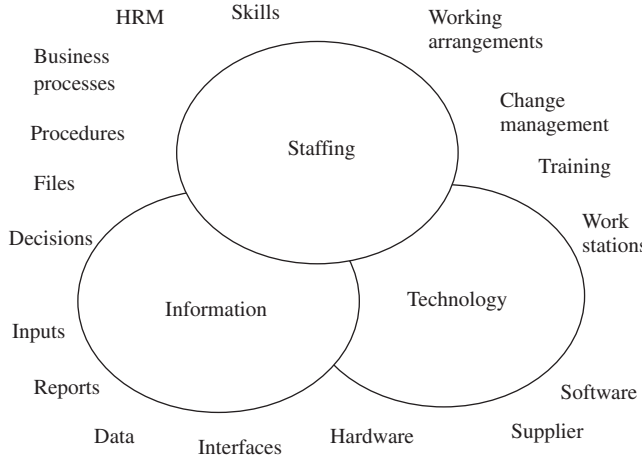


FIGURE 7.26 Three-part SD model.

We expect an SD project to consider the project terms of reference:

Staffing

1. The way staff are deployed.

2. The skills and aptitude of staff.
3. The way the new system is sold to them.
4. The way new working arrangements are determined.
5. The need to rationalize the operational processes, particularly regarding the flow of information files through the processing procedures; also the way information is extracted and delivered to enquirers both within and outside the organization.

Information

1. The type of standard reports required – the decision support system model requires this feature to be flexible and controlled by the user.
2. The type of data that are already available and their general state.
3. The new data that are required and how they might be captured.
4. The extent to which information will be either automated or held on manual files.

Technology

1. The strains and stresses on the system and the capacity required to deal with this.
2. The type of operating system and actual machine configuration that is required.
3. The number of networked terminals.
4. Benchmarking arrangements for the new machine.
5. The interface between the existing IT architecture, including networks and communications.
6. The skills of in-house IT staff and degree of dependency on suppliers.

These three components are interlinked. The staffing/operational issues determine the information solution, which, in turn, determines the technological requirements. Many systems projects have a main focus on the IT part and make passing reference only to the other two at the feasibility stage. The main implementation stage is then driven by the need to get the hardware in place, the data converted and the computer running smoothly, which is component 3. The first two are simply fitted into the project if there is time. More importantly, the project team may not have the necessary skills to deal with high-level human resource management and business process re-engineering problems. The auditor will need to consider these issues since they impact on the likely success of the system. Our view of controls may have to be expanded to take on board these wider concepts in viewing the SD life cycle. A large proportion of control is located in the overall managerial arrangements for a business. This also applies to IT projects and, as such, any consideration of controls must be applied by the auditor within this context. The IS auditor will promote the use of good project management principles. For the audit role in systems development there are two main approaches:

1. **To review the way that the organization controls developments generally** Project management techniques should be applied along with a defined methodology that suits the organization. We are concerned here with the process itself and the way that it is used. To test compliance, a number of actual past or ongoing developments would be selected and examined in order to test the extent to which the defined SD process has been applied in practice. This may be an effective way of using scarce audit resources.
2. **To ensure that audit is present on all major development projects** We would advise on any control implications relevant to the system under development. The audit role would be as watchdogs picking up on any control loopholes. This can be very useful for major,

sensitive systems that are working to tight timetables. Potential control problems could be rectified before it is too late and possible disaster thereby avoided. There is a point of principle that arises here in that it places responsibility for ensuring systems have sound controls in audit's hands. Management is responsible for controls and audit's role is to review and advise on possible control weaknesses. Taking this task away from management, deprives it of an opportunity to acquire a control orientation. In practice, urgent short-term problems call for all parties to get involved in seeking solutions and points of principle tend to be placed to one side. However, it is only by taking a long-term strategic view that the audit role can be directed to the real welfare of the organization. When reviewing either the SD process or individual developments, note that:

- the auditor is one of the system's users and can ask for certain requirements such as an audit-based link into the system or a remote testing facility.
- the auditor must remove the mystique behind computing: basic project management techniques are applicable to all types of development regardless of the level of technical complexity.
- audit may be seen as 'wet blankets' who look for problems rather than become caught up in the excitement of 'making the system work'.
- an embedded audit module may be built into the new system and allow unrestricted access to files for audit testing (note that this does cost money).
- audit independence should be watched and it should be made clear that involvement in systems development work does not mean that the system now belongs to internal audit.
- the amount of testing that audit will perform should fit into the systems development plans and audit should be careful not to unreasonably hold up progress.
- there is some debate as to whether the auditor should 'sign off' the system before it goes live: it is not the auditor's system but at the same time the auditor does have a professional obligation to give an opinion when asked, without assuming operational responsibilities.
- if the auditor acts to check on the work of the project team this may lead to the auditor being perceived as a negative force, perhaps as some type of management spy.
- the auditor should have sufficient training before tackling a complicated development; newer auditors may rely on the goodwill of IS staff, which depends on the relationship with the IS manager.
- there is a link between audit and quality assurance and if there is a suitable quality programme for systems development that is arranged by the IS department, this should receive audit attention; if quality assurance works, this acts as a major control over the development process.
- controls cost money and time and the auditor should appreciate that all systems have a 'Rolls-Royce' control option and a more realistic one; the organization cannot operate a zero-risk policy for all operations and a business-like approach must always reign – the criterion should be that controls should be adequate and effective.
- auditors need to go through familiarization before any systems development is reviewed and systems documentation should be obtained and reviewed beforehand.
- an important role auditors may adopt is to present a series of searching questions to external consultants who may be managing the projects – consultants work on individual projects within an agreed fee budget and not necessarily for the welfare of the organization.
- audit input into individual projects may uncover weaknesses in the SD process.

Audit must be involved in the development process, although the nature of this involvement will depend on the audit and the organization's policies. Whatever the role, it should be well defined and publicized.

The IS auditor does not lose independence by performing tasks such as:

- reviewing controls;
- testing compliance with standards;
- providing advice on control techniques;
- promoting the use of project management;
- determining whether security standards are sensible;
- advising on the management of systems performance;
- helping management identify and address relevant risks;
- helping to identify project roles.

Involvement over and above these tasks will tend to fall under the consulting role of the IS auditor. Note that audit independence was dealt with earlier in the handbook.

The Importance Of Auditing IT Projects Well

By Dan Swanson, Compliance Week Columnist

Changes to a company's IT infrastructure are a significant source of risk for every business; to protect the corporate crown jewels, robust change-management practices are absolutely critical. The need for a positive ''control environment'' within IT and a very unforgiving attitude regarding unauthorized IT changes cannot be overstated. In fact, a recent study by the IT Process Institute indicates that ''best of breed'' IT shops outperform their counterparts by a huge margin on many different performance indices. The two controls that were almost universally present in these high performers were:

1. Monitoring systems for unauthorized changes; and
2. Having defined consequences for intentional, unauthorized changes.

Internal audit's role regarding the implementation of IT initiatives varies widely, but also provides a significant opportunity for internal audit to deliver real value to the board and executive management. That is, internal auditors should play an important role in ensuring that IT investments are well-managed and have a positive effect on an organization. A well-managed IT project is absolutely critical to this success. IT efforts are getting more complicated each year; operational changes are becoming more challenging with each new technology being adopted, particularly where global operations are now being supported. The system integration requirements continue to amaze even the most experienced IT and audit professional.

An audit of an IT initiative can take many forms. At its simplest, the auditor can review the business case and hold a few interviews with key stakeholders. At its most complex, a full-time audit team will participate in almost every aspect of the IT project. This diversity depends on the risks involved and the assurance requirements of the board and executive management. If the organization would totally unravel if the IT initiative fails, a ''health checkup'' by internal audit can be very worthwhile.

Auditing Major IT Initiatives

The board and management want to know many things regarding their IT efforts: that the IT efforts are productive, that the IT investments will have an impact, that their

system of internal control is enhanced and strengthened by their IT efforts, and that the next disaster (from a failed IT implementation) will not happen. An independent assessment of an IT initiative can provide that feedback and prevent trouble down the road or perhaps even prevent a business failure. Defining the audit goals, objectives, and scope for a review of an IT initiative is a key first step. The internal auditors' involvement with an IT initiative typically involves reviewing and assessing the overall project plan and project management. Auditors also need to assess the accuracy and completeness of the systems and data requirements for the proposed IT solution, by:

- Evaluating and monitoring management's project plans for the various system changes that will be required;
- Assessing the completeness and appropriateness of management's systems and database design, including security and privacy aspects;
- Reviewing the user-acceptance and parallel-test planning and results to demonstrate successful end-to-end system operations and the ''preparedness'' for implementation (in a parallel test, the project team simultaneously tests both the old and new systems using the same data and compares their results in a comprehensive manner); and
- Reviewing the startup of production systems and associated client data to ensure data integrity is maintained and ''back out'' plans in the event of a problem will be effective.

In addition, auditors need to assess the accuracy and completeness of the startup of operational responsibilities within the organization (for the new IT ''solution'') by:

- Evaluating and monitoring management's project plans for the various operational requirements; and
- Assessing the completeness and appropriateness of the operational policies and procedures that are developed, and the related training.

The organization's various IT initiatives cover a broad span of technologies and just as importantly, they affect business operations in a variety of ways. The planning phase of the audit needs to ensure the proper focus of the audit efforts. Internal auditors need to determine the level of their involvement and the best audit approach to take (during the IT initiative's initiation phase). The audit involvement decision should be based on the audit-risk assessment, and include factors such as the team's project-management experience, level of management involvement, size and complexity of the initiative, and effect on the organization if the initiative is delayed or unsuccessfully implemented. The most appropriate audit approach also needs to be defined during the audit project-planning phase.

Key issues to explore during the audit include: effective project sponsorship and project management (two absolutely critical factors in every IT project), accuracy of the business requirements, representation of all stakeholder groups on the team, and the existence of a robust IT risk management process.

Encouraging Better Performance

Like most audits, the audit of an IT initiative generally will involve three phases: planning, fieldwork, and audit reporting. IT initiatives, however, come in many

shapes and sizes, so the audit of an IT initiative must be flexible and risk-based. During the planning phase, the internal-audit team should ensure that all key issues are considered, that the audit objectives will meet the organization's assurance needs, and that everyone involved understands the IT initiative that is being audited. It is important that the audit focuses on evaluating the significant components of the IT initiative – to use a risk-based approach to find the project elements most likely to fail or most in need of confirmation. The planning phase also should confirm that the audit scope is appropriate.

In the fieldwork phase, the auditor analyzes the IT initiative's various components based on the goals and methodology identified in the planning phase. Among some of the most important questions to answer are:

1. Have the business requirements been clearly defined?
2. Will the IT solution meet those requirements?
3. Has the IT solution been proven to work?
4. Is it secure and will privacy of information be maintained?
5. Has the amount of effort involved reflected the risk involved with the solution's implementation?

Audit tests could include reviewing business-case documentation and system-related documents; interviewing key participants in the project; looking at training materials and development of procedures for the solution's operation; and reviewing test plans, their results, and management's communications to employees regarding preparation for implementation. The audit-reporting phase is where the internal auditor ensures that all stakeholders are informed of the audit results and management's plans to enhance the IT initiative's efforts. Audit reporting can be straight forward: Tell them what you did, what you found, and what management plans to do.

The difference with auditing an IT initiative is that audit feedback needs to begin as early as possible, so change in project plans and efforts can be considered. Therefore, formal, ongoing feedback should be provided to the management of the IT initiative, and senior management and even the audit committee on occasion should be briefed with periodic status reports. Formal end-of-audit reporting is still needed, but any ''news'' from the audit team must be conveyed long before the audit report is formally issued.

We Need To Encourage IT Process Improvement

Auditing best practices recommend that internal auditors should be involved throughout an IT initiative's life cycle, not just in post-implementation evaluations (where the wounded are shot). An internal audit of an IT initiative also needs to be part of a broader IT audit plan as one audit does not assess the IT function's overall performance. It is a long-term assessment of IT efforts where true IT process improvement can be encouraged. For example, does the organization have a robust IT risk-management process? Is IT implementing comprehensive patch- and change-management practices? Has the development and implementation process been updated to reflect today's significant security and privacy requirements? Is there an overall organizational project office?

Auditors can bring considerable value to an organization by evaluating both the IT and organizational aspects of an IT initiative. Because a conversion to a new IT solution is one of the highest risks that an organization can face, internal auditors' involvement and independent assessment of the issues and project plans will provide value far in excess of the audit's costs.

Reprinted from *Compliance Week*. This article was originally published in Compliance Week. Reproduced by permission of Compliance Week. All rights reserved.

Information Systems Security

The internal auditor should periodically assess the organization's information security practices and recommend, as appropriate, enhancements to, or implementation of, new controls and safeguards. Threats such as computer fraud, espionage, sabotage, vandalism and natural disasters can bring down the corporate network and damage important databases. The ISO standard 7799 addresses IT security and has the following sections:

1. Business continuity planning
2. System access control
3. System development and maintenance
4. Physical and environmental security
5. Compliance
6. Personnel security
7. Security organization
8. Computer and network management
9. Asset classification and control
10. Security policy.

Much of the classification of information systems is based around risk assessment in terms of the impact on the business. Moreover, ISO 7799 recommends that audit requirements and activities involving checks on operational systems should be carefully planned and agreed upon in order to minimize the risk of disruptions to business processes and suggests the following be observed:

- Audit requirements should be agreed on with appropriate management.
- The scope of the checks should be agreed on and controlled.
- The checks should be limited to read-only access to software and data.
- Other types of access should be allowed for isolated copies of system files, which should be erased when audit is complete.
- Requirements for special or additional processing should be identified and agreed on with service providers.
- All access should be monitored and logged to produce a reference trail.
- All procedures, requirements and responsibilities should be documented.

The ISO standard (7799) goes on to list several key controls that support the security infrastructure:

- Information security policy document
- Allocation of security responsibilities
- Information security education and training

- Reporting of security incidents
- Virus controls
- Business continuity planning process
- Control of proprietary copying
- Safeguarding of company records
- Compliance with data protection legislation
- Compliance with security policy.

The growth in e-business makes encryption, third-party access and rules on remote or teleworking important as controls must keep pace with new developments.

Educating Staff Leads to Improved IT Security

By Dan Swanson, Compliance Week Columnist

In today's business environment, information security and protection of information assets are vital to the long-term success of all organizations. Information is the lifeblood of corporations and a vital business asset. IT systems connect every internal department of a company and connect the whole company to myriad suppliers, partners, customers, and others on the outside, too. Still, problems with IT – from system failure to data breaches to improperly altered applications – happen almost every day. Security breaches in particular can be disastrous for a company. And most companies do not adequately address the primary cause of IT security breaches: human error. In this article, I explore how workforces should be educated about IT security and how to determine whether they ''get it.''

Rating Your IT Security Program

How do you get started figuring out how well your company performs on information security? This checklist will get you started:

- Has your organization implemented a comprehensive information security program?
- Does your organization have robust and effective information security policies, procedures, and controls? Are they enforced?
- Does management promote an ethical culture? Would you say your workforce follows management's lead to create a strong ethical culture?
- Does the information security program reflect the risks and complexity of the organization? Are risk assessments occurring?
- Does the program actively identify new ways of protecting the organization from harm based on emerging threats?
- Are the security measures and controls regularly tested for operational effectiveness, and are corrective actions occurring?
- Are your information security and privacy training effectiveness measured throughout the entire training lifecycle?
- Is performance being measured and reported to senior leadership and other key stakeholders?
- How does the organization's security compare with other well-run similar organizations?

- Was your security program evaluated in the past 18 months?

If you answered ''yes'' to all the above questions, congratulations! You're well on your way to an effective and sustainable information security program. Now, answer four more questions that will help move you to the head of the class:

- Does your program include ongoing security awareness?
- Do appropriate staff members get security education appropriate for the jobs they perform?
- Do members of the management team and workforce understand what good security practices are? How do you know?
- Are you assessing and measuring the results of your security education and awareness efforts?

The Role of Internal Auditors

An effective internal audit function improves the company's ethical culture and control environment, both overtly through its audit work and in a more general sense by promoting good practices. Internal audits of information security awareness can provide valuable feedback to management and the board about where overall performance can be improved, which then also contributes to more effective information security program results – definitely a win-win.

Audit work should include evaluating the organization's various security education and awareness efforts. If management and staff are not being regularly informed of emerging threats and risks, how can security be properly implemented on a sustainable basis?

An audit should compare good security practices to what is currently happening within the organization and review the results too. In other words, is quality training being provided, and is real learning happening?

Staff Involvement

Education is the formal training class that a system administrator might attend to learn how to better apply Microsoft Profiles to controlling changes to the desktop. Awareness is the program that a company puts in place to remind employees with repetitive procedures (and at least an annual update in person) of policy, procedures that support policy, and practices they must know to comply with company policy. Awareness is both formal and informal. ''Formal'' is the 20-minute annual awareness session; ''informal'' are excerpts in company newsletters, security awareness e-mails, and reminders of special days such as Global Security Awareness Week.

A good method to deliver that security awareness message to the workforce is first to educate them on the actions they can take to protect themselves personally from the issues that face individuals today. These include such things as identity theft, phishing attacks, and proper precautions to take when sharing personal information online. Provide this information in the training sessions; make the process personal. More security education and awareness practices are presented below; numerous others are available in the resource sidebar.

1. Regularly provide updated threat information to management and staff. Some common concerns today include: password theft, laptop theft, infected e-mails, ''shoulder surfing,'' and dumpster diving. With clear communication channels that allow everyone to be more informed on the latest threats, and changes in previous threats, it encourages the workforce to be better prepared and to consider new security measures where beneficial. Many times, an educated and motivated workforce is your best defense.
2. Explain the possible consequences of security incidents in business terms. Your company or its workers could endure identity theft, equipment theft, loss of productivity, loss of competitive advantage, increased staff turnover, penalties due to compliance fines, loss of reputation, loss of data, and eroded customer confidence. While the list is long, the workforce absolutely must know what the effects on the business could be. By making it ''personal'' and demonstrating the possible hit to operations, increased support for good information security practices can be ''reinforced.''
3. Provide comprehensive, role-based courses to select management and staff who require the latest knowledge regarding good security practices. Here, the issue is ensuring that an investment in skills and staff competencies is happening on a regular basis. There is nothing worse than not knowing something you think you do know.
4. Regularly provide best-practice information for various IT security and IT management processes. Some important processes include: patch and change management, configuration management, security design and architecture, fraud prevention and detection, physical security – and there are many more. Explain not just the ''how,'' but the ''why'' of various security processes and procedures to staff. And a wise first step is to focus on educating ''the influencers'' of your management and staff ranks, and then let them set the example for the rest.
5. Complete periodic surveys of management and staff. This is to assess how well they understand the information security policy, procedures, and controls as well as to identify key opportunities for improvement. Communication is a two-way street, and if you never assess staff competency you'll never know how well your staff development efforts are going. Surveys are a low-key method of finding out what's on the minds of people and what training issues need to be addressed.

While these steps aren't necessarily inexpensive and your company will always have limits to its education budget, over the long haul these are low-cost investments with a high-benefit payoff: peace of mind about your information security.

Regular Evaluations

Setting clear expectations and defining everyone's responsibilities for IT security is half the battle. Being diligent in your efforts to be sure the workforce understands the organization's expectations and their roles and responsibilities is the other half. To implement proper security, you need an articulate policy, it must be enforced, and violators must be investigated and punished when necessary. Management must understand that it has a responsibility to design and implement information security education and awareness activities, including the monitoring of those results.

Management and staff need to be assigned security responsibilities, and their compensation increases should include assessing their security ''performance'' as well as the more traditional criteria for setting pay. Holding management and staff accountable for their performance regarding information security is key to effective security. (It's called ensuring ''consequences'' for people's ''actions.'')

Awareness should take multiple forms, such as company newsletters or impromptu forums. The effectiveness of any such effort also depends on the tone set by senior management.

The best defense against security incidents and failure is having a ''motivated'' and educated management and workforce to support your organization's IT security standards. Many things can happen due to lack of awareness and education, from lost customer confidence to lost customers, as well as lower stock prices, lawsuits, bad publicity, and more. The list is endless. Building awareness of information security takes time, resources, and energy, but without question, it's worth it.

Reprinted from *Compliance Week*. This article was originally published in Compliance Week. Reproduced by permission of Compliance Week. All rights reserved.

Disaster Planning

The type of information lost and the length of the interruption will have an impact on the extent of damage done. Some of the disasters that an organization might face include:

Terrorist attacks	Sabotage
Strike	Fire and explosion
Natural disaster	Systems failures
Corrupt database	

Disaster planning is about preparing for these and other undesirable events which may affect the share price, sales income, orders, suppliers and other matters that affect the reputation of an organization. The normal disaster planning process is set out in Figure 7.27.

How To Audit Business Continuity Programs

By Dan Swanson, Compliance Week Columnist

Being able to continue critical business functions while responding to a major disaster, and then to return to normal operations efficiently and cohesively afterward, is a critical success factor for all organizations. Effective business continuity (BCP) and disaster recovery (DR) programs are vital and have become a necessary cost of doing business. They must receive adequate attention and support from management if the company is to survive and remain competitive in a post-disaster situation. The purpose of these programs is to prepare the organization to cope more effectively with major disruption. Program managers plan possible responses in advance of the actual incident(s) rather than simply responding in the heat of the moment. This planning increases the quality and consistency of the response regardless of the person who executes the plan. The programs must cope with a wide variety of potential incidents, from man-made disasters such as power-grid or other critical infrastructure failures to natural disasters such as hurricanes, floods, or fires. Simple incidents also can have huge consequences, so don't under-plan; for example, expect that your staff won't make it to work due to an ice storm. It is an unfortunate fact of life that, despite our

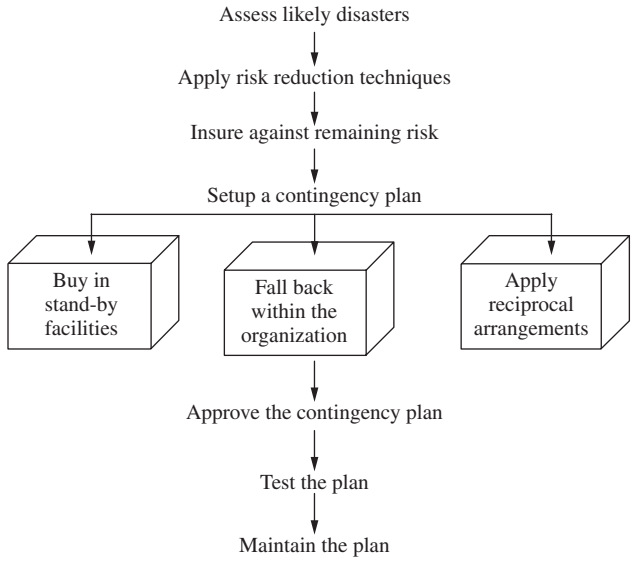


FIGURE 7.27 Disaster planning process.

best efforts, some disasters are simply unavoidable. The quality of an organization's response to such a crisis can make the difference between its survival and its demise.

Because the BCP and DR efforts are so important, they should each fit together hand-in-glove.

Internal Auditing's Role In BCP And DR

Internal audits of the BCP and DR programs are highly recommended. The board and management need assurance regarding the effectiveness of those efforts. They want to know that the DR plan will work when needed, that the investments in BCP and DR are obtaining good value, and that a disaster will not bring the business to its knees. An independent assessment of the BCP and DR programs by internal audit can provide objective feedback that helps ensure the programs are adequate to prevent a business failure. Think about it: While everyone has focused on the requirements of Sarbanes-Oxley for almost five years, have your DR and BCP efforts kept pace with today's new challenges and expanding requirements? Have an answer, because your board is increasingly likely to ask. Exactly how internal-audit departments should interact with BCP and DR programs varies widely among companies. With the right approach, audit can deliver real value to the board and executive management by objectively assessing whether the program provides effective coverage to protect the organization from harm when a significant disaster occurs.

An audit of the BCP and DR program can take many forms. At its simplest, auditors can conduct a quick ''BCP/DR health check,'' reviewing the plans and interviewing key stakeholders. At its most complex, the audit team can analyze almost every aspect of the program, evaluate the risk-based planning, observe BCP/DR tests, assess the completeness of the business-impact analysis, and so forth. The type and the extent of auditing performed depends on the risks involved, management's assurance

requirements, and the availability of audit resources. External specialist resources may be useful on occasion. The auditors might participate as formal observers in mock drills or review the program's documentation and assess its comprehensiveness and completeness. Your options are numerous.

Internal auditors normally will review what has been planned and achieved against management's expectations and in comparison to generally accepted best practices in the field. This is where audit objectivity comes to the fore; the auditors have a legitimate purpose to assess whether management's expectations are reasonable and sufficient, given the level of risk to the organization and in relation to other similar organizations. The following advice covers the main phases of any audit: scoping, planning, fieldwork, analysis, and reporting. BCP and DR programs, however, come in many shapes and sizes, so clearly the specific details of any given audit will vary according to the situation.

Audit-Scoping Phase

As with any audit, defining the goals and objectives for a review of the BCP and DR programs is the auditor's first task. Scoping is best conducted on the basis of a rational assessment of the associated risks. The following aspects are generally worth considering when scoping a BCP and DR audit:

- ***Overall Program Governance.*** How are the programs managed? Are they given appropriate strategic direction and investment? (That is, does the organization place sufficient emphasis on BCP and DR?) Are suitable sponsors and stakeholders involved, representing all critical parts of the organization? Do they take sufficient interest in the programs, demonstrating their support through involvement and action? And most importantly, who is accountable for their success or failure?
- ***Ongoing Program Management.*** A critical success factor in every BCP and DR effort is the way in which the programs are planned and driven to ensure that they meet objectives despite the organization's inevitable competing priorities. Does program management balance consideration of the many conflicting priorities managers face with the critical need that corporate resiliency efforts be appropriate? This is not a once a year exercise anymore; being prepared is an ongoing, day in and day out effort.
- ***Definition And Accuracy Of The BCP And DR Objectives.*** Have the programs' requirements been clearly and fully defined by management? Has a comprehensive business-impact analysis been completed? Is it regularly updated?
- ***Coverage Of The BCP And DR Plans.*** Have all the critical business processes been identified and suitable plans prepared? Do the plans take sufficient account of the need to maintain or recover the supporting infrastructure (IT servers and networks, for example)? Are the plans reasonably ''tidy'' or are they cluttered with non-essential processes, systems, and activities? Are significant outsourced activities adequately covered? Do they need validation as well?
- ***Management Of Any System Or Process Changes.*** Inevitably, changes will be required to implement BCP and DR arrangements. Is change management managed effectively to provide the best assurance that changes are tracked and addressed within the live and DR environments?

- ***Robustness Of The BCP and DR Testing Processes.*** Program managers need to demonstrate the organization's preparedness, build management confidence, and most importantly, strengthen the organization's BCP and DR capabilities; Is ''people participation'' identified, approved, and tracked to provide the best assurance that the drills and tests are actually attended, and that those results meet your BCP and DR objectives?
- ***Plan Maintenance.*** How is the change-management process that keeps the plans up to date governed, even as the organization changes? Are roles and responsibilities allocated within the organization for developing, testing, and maintaining BCP and DR plans?
- ***BCP And DR Procedures.*** Consider the procedures and associated training, guidelines, and so forth to make managers and staff familiar with the process to follow in a disaster.

In addition to defining what aspects fall within the audit's scope, equally important is that management and the board clarify any aspects that are out of the scope – particularly any important considerations that, for one reason or another, are not going to be covered at this time (say, perhaps because they will be audited separately). A natural part of the scoping phase is to identify one or more management sponsors for the audit. Audits are conducted for the benefit of the company's management rather than for audit's own purposes, so it is important to know who will receive, accept, and act upon the final audit report. Their overt support for the audit can make audit's job much easier, such as by engaging and gaining the involvement of suitable auditees.

Audit-Planning Phase

Having defined the scope, the audit team needs to plan the audit within the constraints of available resources from the audit department and from the business as a whole. Resourcing decisions are largely risk-based, taking account of factors such as the program management's experience, the level of management involvement in the program efforts, the size and complexity of the program, and the potential effects on the organization if the program fails.

The availability of suitable auditors is, of course, a prerequisite. Audit teams combining business and IT auditors are recommended wherever possible, since BCP and DR span both fields of expertise.

This is also a good time for the auditors to identify and contact the primary auditees. Securing their assistance with the audit fieldwork is easier if they have an opportunity to comment on the timing and nature of the work required – provided that the audit department's independence and objectivity are not unduly compromised in the process! The audit approach also needs to be decided during the audit planning. For instance, will it be feasible to review all BCP and DR plans, or is it necessary to sample the plans? If so, on what basis will the sample be selected? Should auditing of BCP and DR efforts be separate and distinct audits? (For many organizations this could make sense, as they are both important activities worthy of a focused and comprehensive review.) Does auditing of outsourced activities and related BCP and DR plans need to be completed?

Most auditors generate an audit checklist at this stage, converting the agreed audit scope into a structured series of audit tests that they plan to conduct. Styles vary, but the most useful checklists aim to guide (rather than constrain) the auditors, since the extent of the audit testing required depends somewhat on what is found. Researching what's available regarding an audit program is, as always, recommended. And of course, before fieldwork commences, audit management should review the audit plans and checklists to ensure that all of the key issues identified in the scope have been given sufficient consideration to satisfy management's assurance needs.

Audit-Fieldwork Phase

In this phase of the audit, the auditors examine the BCP and DR program based on the goals and methods decided upon in the earlier phases. BCP helps the organization to survive a disaster by keeping critical business processes operating during the crisis, whereas DR restores the other less-critical processes following the crisis. Audit testing during the fieldwork phase gathers sufficient evidence to assess whether the program is able to meet these two fundamental requirements. Audit tests of a BCP and DR program may include the following:

- Interviewing key stakeholders and participants in the program;
- Reviewing business case-, planning-, and IT-related documents;
- More or less detailed reviewing of individual BCP and DR plans, checking that they are complete, accurate, and up-to-date – for example, testing a sample of the contact details for key players to confirm whether their phone numbers are correct;
- Looking for defined recovery times and whether there is evidence that they can be met;
- Examining training materials, procedures, guidelines, and so forth, plus any management communications regarding BCP and DR situations that might occur and what employees should do;
- Reviewing testing plans and the results of any tests already conducted;
- Evaluating relevant employee preparedness and familiarity with procedures;
- Reviewing impact of new regulation on plan; and
- Reviewing contractor and service provider ''readiness'' efforts.

Details of the tests are normally recorded in the audit checklist. They are accompanied by a file containing the corresponding audit evidence, such as annotated copies of BCP and DR plans, test results, and other materials that the auditors have reviewed.

Audit Analysis And Reporting Phase

Audit reporting is a straightforward process, at least in theory. This is where the auditors analyze the results of their tests, formulate their recommendations, prepare, and finally present a formal audit report to management. In the report, the auditors explain:

- ***What they set out to do.*** This part of the report will introduce the risks and recap the audit scope;
- ***The audit methods.*** This will describe how the auditor went about meeting the objectives;

- ***What they found.*** This typically covers the key issues identified, if not the full gory details. Not all findings are reportable, but sometimes it helps to provide the completed audit checklist as an appendix to the report and invite management to review the audit evidence if it wants more information; and
- ***The recommendations.*** This will entail advice to management on how to address the issues identified.

In practice, audit reporting varies widely among organizations. It requires a careful balance between the somewhat idealistic outlook of some auditors and the realities of managing the organization with limited resources and competing priorities. There is usually a fairly involved, iterative process of drafting, reviewing, and correcting the report and negotiating the details with management to reach the best possible outcome for the organization. At the end of the day, it is management – not the auditors – that is responsible for deciding which, if any, recommended improvements to the BCP and DR program they intend to make. The audit process has the advantage of systematic collection, testing, and evaluation of audit evidence by an independent yet interested function. The facts of the matter carry a lot of weight with management. The audit report should present the purpose and objectives of the audit, the audit approach, and test performed, the key opportunities for improvement, as well as detailed findings and management's action plans. A description of the actual BCP and DR program including its scope, mandate, role, and accomplishments also would be useful in getting everyone on the same page regarding organizational investments in BCP and DR efforts.

Investment In Resiliency

Auditors can bring considerable value to an organization by evaluating both IT and organizational aspects of the BCP and DR program. Because failure of the BCP and DR programs when needed is one of the highest risks that an organization can face, internal auditors' independent assessment of the program will provide value far in excess of the audit's costs. Management always should be looking for ways to improve its BCP and DR program efforts – that is, don't just wait for an audit. Involve internal audit in your ongoing program efforts, such as the design and execution of a testing exercise. Regular management ''self assessments'' should be encouraged, and comprehensive testing of the program is always strongly recommended.

Companies need to take a boardroom perspective for their BCP and DR program efforts. What absolutely must be in place to ensure the organization's survival? And do you have the plans and programs in place to deal with a significant disruption to operations? (Including assigning responsibilities and accountabilities for business continuity efforts, and providing the program with the necessary resources to deliver when needed.) The bottom line is whether your investment in resiliency is appropriate. What measures have been implemented to track your progress? And, finally, is management regularly assessing and improving the organization's ''preparedness'' capabilities in the event of a disaster?

Reprinted from *Compliance Week*. This article was originally published in Compliance Week. Reproduced by permission of Compliance Week. All rights reserved.

Standby Facilities

The organization should ensure that it has a contract for standby facilities to take over processing in the event of the computer centre becoming unusable. There may be three main different types of standby contracts:

1. **Cold standby centres.** One might either:
   - maintain an in-house facility into which servers might be moved or
   - subscribe to an existing facility.
2. **Warm standby centres.** Here the facility would be readily available and be functional within a fairly short time.
3. **Hot standby centres.** This facility, being the most expensive method, is set up with copies of the files dedicated to the system in question and may be operational at a moment's notice.

Hot and warm centres may be provided by a suitable supplier and again the response rate will depend on the degree to which processing is critical to the organization.

Whenever a disaster occurs, consideration should be given to contacting each of the relevant parties and one may establish a formal disaster committee that has been well briefed and rehearsed. The resources expended in recovering the information will depend on many factors since the information may be critical, important or merely useful. Relevant factors are:

Restoration speed	Frequency of use
Relative importance	Cost of recovery
Impact of legislation	Available recovery method
Sources of information	

The standard disaster plan should cover items shown in Figure 7.28.

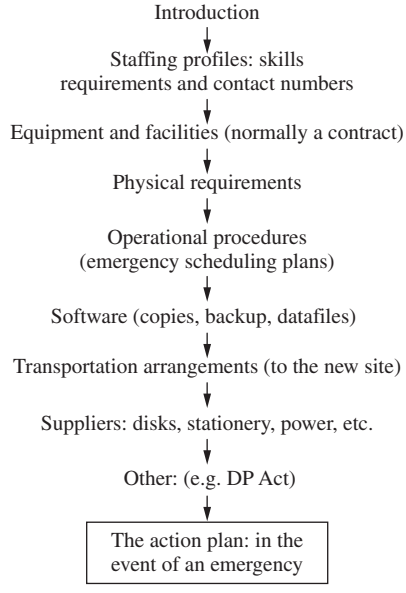


FIGURE 7.28 Disaster plan.

The Disaster Coordinator

It is necessary to appoint a disaster coordinator to devise the plan, test it and oversee arrangements. This requirement should be built into the job description of the IS manager and form part of performance appraisal. The disaster action plan should be tested periodically and participants should meet at least once a year to discuss current arrangements and issues. The plan should be directed primarily at high-priority systems that have been identified through a formal process of risk assessment. The IS auditor's role in disaster planning is to:

- recommend that a plan is in place;
- independently test this plan;
- review the contract with the facility's supplier along with any tendering arrangements;
- review the extent to which the plan is understood by all participants;
- advise the disaster committee on any security implications that may need to be addressed.

In any emergency, operational expediency tends to take precedence over control matters and short cuts may be taken by management. The principal control in this situation is the presence of key officers who can be responsible for authorizing any required action. This may include the release of large creditor system cheques from a remote standby location, or, for that matter, handwritten cheques. Another key consideration is the way responsibility is located throughout the organization. The IS manager should be required to establish a contingency plan. The participants will include those who authorize use of important applications such as payroll, creditors, and income systems. With distributed systems, many applications are controlled by end users who should be represented on the disaster planning committee. To force decisions on roles and responsibilities, there must be a higher level forum that would drive the plan linked into the executive decision-making mechanism, led by the chief executive. It is good practice for internal audit to present reports to this forum which may be a high-level IS steering group. Another technique is to ensure the audit committee is made aware of anything that may impair the emergency arrangements. In times of financial constraints, subsidiary matters such as disaster planning may take a back seat. This does not mean that disasters will not occur and the systems for managing them should be subject to audit cover. The IIA.UK&Ireland's guide to *IT Disaster Recovery* confirms current best practice by suggesting a checklist of aspects to be considered by the auditor during a review of the contingency and disaster planning processes:

- Does the organization take contingency planning seriously and is this demonstrated by board/top management commitment?
- How have responsibilities been assigned to this activity?
- Has a risk-based approach been used to identify key systems and priorities for recovery?
- Has the organization considered preventative measures to reduce the risk of a disaster and are these considered appropriate to the risk?
- Have the recovery options been considered in the case of a major disaster and have these been documented in a written contingency planning and disaster recovery plan?
- Is an appropriate degree of testing carried out and is the output of testing used to improve the plan?
- Have appropriate procedures been established for the maintenance and updating of the plan?
- Are copies of the plan and any other significant documentation held securely?[49]

Operational Resiliency: The Next Business Priority!

By Dan Swanson, Compliance Week Columnist

Ensuring that an organization can recover from disaster is a basic business requirement the board should explore regularly with management. Nowadays, leading companies are taking this requirement and turning it into a strategic advantage: Namely, investments in operational resiliency are assisting organizations to become more responsive to client needs as well as improving operational reliability, quality, and efficiency. It's an effort you should embrace, too. Operational resiliency covers a huge waterfront, and a universally agreed-upon definition of it continues to be elusive. To some, its focus is purely on IT recovery capabilities, where investments in network and software redundancy are the priority. For others (usually business managers), it means strengthening the business unit's recovery capabilities, which brings a focus to business continuity plans. For still others (senior executives and board members), it's the organization's ability to respond to emergencies and meet client needs. I believe operational resiliency covers all of the above.

As companies face increasingly complex business and operational environments, functions such as security and business continuity keep evolving; indeed, they need to keep evolving. Today, successful security and business continuity programs (BCP) both address the technical issues involved and strive to support the organization's efforts to improve and sustain an adequate level of operational resiliency. Operational resiliency efforts tackle operational risk by identifying potential operational problems and improving the processes and systems used; that is how operational problems are reduced over the longer term.

Being able to continue critical business functions while responding to a major disaster, and then to return to normal operations efficiently and cohesively afterwards, is a critical success factor for all organizations. Effective business continuity and disaster recovery (DR) programs are vital and have become a necessary cost of doing business. They must receive adequate management attention and support if the company is to survive and remain competitive in a post-disaster situation. The purpose of the BCP and DR programs is to prepare the organization to cope more effectively with major disruption. Business managers plan possible responses in advance of the actual incident (or incidents), rather than simply responding in the heat of the moment. This planning increases the quality and consistency of the response – that is, it makes the operation resilient to disruption – regardless of the person who executes the plan.

Taking this effort to the next level, management needs to enhance its operational culture, processes, and systems, by strengthening the reliability and efficiency of each. An organization's operational resiliency program should be an umbrella effort; that is, it should provide support and guidance for the organization's information security, BCP, DR, and emergency management program efforts. The following questions should be considered as part of any effort to improve operational resiliency:

- Are security and business continuity activities planned in a coordinated manner in your organization, or are they performed in silos? Are they viewed as technical rather than business activities?

- Can you actively manage operational resiliency, or do you typically react to disruptive events as they occur?
- Do you know if the security and business continuity practices you've implemented are effective? Have you tested them? Do they support the achievement of the organization's strategic objectives and mission?
- Can you measure the success of your security and business continuity activities? Can you consistently repeat and sustain that success over the long run? Have you benchmarked your activities against others in your industry, or against independent third-party guidelines?
- Do you have a foundation from which to continuously improve your security and business continuity efforts?

Internal Auditing's Contribution

Internal audits of information security, BCP, and DR programs are highly recommended, and as mentioned, have been covered in previous columns. The board and management need assurance regarding the effectiveness of those efforts, and they also need assurance that the company is building a more efficient and effective operation. During every internal audit project, auditors should consider including an evaluation of the business unit's efforts to be more efficient and effective, and in particular what initiatives are being implemented to enhance operational resiliency. Over time, internal audit's focus on assessing management's efforts to make operations more reliable will support the company's efforts to improve enterprise-wide processes and systems. The following aspects are generally worth considering when scoping an audit of operational resiliency efforts:

- ***Overall program governance.*** How is operational resiliency being encouraged? Is the program given appropriate strategic direction and investment? (That is, does the organization place sufficient emphasis on operational improvement?) Are suitable sponsors and stakeholders involved, representing all critical parts of the organization? Do they take sufficient interest in the program, demonstrating their support through involvement and action? And most important of all, who is accountable for the programs' success or failure?
- ***Ongoing program management.*** A critical success factor in every BCP and DR effort is the way in which the programs are planned and driven, ensuring that they meet objectives despite the company's inevitable competing priorities. Does program management balance consideration of the many conflicting priorities managers face with the critical need that corporate resiliency efforts be appropriate? This is not a once-a-year exercise anymore; being prepared is an ongoing, day-in and day-out effort.
- ***Management of system or process changes.*** The evaluation of operational resiliency inevitably results in system and process improvement. Is change management handled effectively to provide the best assurance that improvement results are beneficial and that operational reliability is occurring?

A Long-Term Investment

Companies that want to implement a culture of continuous improvement should focus on improving the operational resiliency of key systems and processes. Internal audit should reinforce this goal by evaluating both the whole enterprise's and the individual business units' efforts to address operational risk by enhancing operational processes and systems. Building the resilient organization takes a long-term view and a persistent investment of management's time and resources, and leading organizations are doing this. Finally, being aware of what is important to your customers is critical to your success.

Reprinted from *Compliance Week*. This article was originally published in Compliance Week. Reproduced by permission of Compliance Week. All rights reserved.

Data Protection

The Data Protection (DP) Act 1998 means that the 1984 DP Act now applies to manual data as well as data held on computer. The eight principles under the DP Act 1998 are as follows:

- **First principle.** Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless certain conditions are met.
- **Second principle.** Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
- **Third principle.** Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- **Fourth principle.** Personal data shall be accurate and, where necessary, kept up to date.
- **Fifth principle.** Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or for those purposes.
- **Sixth principle.** Personal data shall be processed in accordance with the rights of data subjects under this Act.
- **Seventh principle.** Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- **Eighth principle.** Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedom of data subjects in relation to the processing of personal data.

The individual's rights under the legislation are listed:

- right of access
- right to prevent processing likely to cause damage or distress
- right to prevent processing for direct marketing
- right in relation to automated decision-making
- right to compensation
- rectification, blocking, erasure and destruction
- requests for assessment.

The subject may be asked to pay an access fee set by the organization and the subject may complain to the Registrar. The DP Act uses terms that have precise meaning:

- **Data user –** this is the party who holds the data.
- **Processing –** this includes amending or deleting the data.
- **Personal Data –** this covers data from which a living individual may be identified. It includes an expression of opinion, for example, X is a bad debt, but not a statement of intent, for example, 'We will not be giving credit to X.'

Meanwhile, there are several exemptions from access, and personal data may be accessed in certain circumstances:

For national security	For the national interests
For tax collection	Department of Social Security records
Research statistics with no names	With the sanction of the Home Secretary
For back-up purposes	Legal and professional privileges
Unincorporated clubs	For accounting purposes
For pay and pensions	

Personal data may be disclosed in certain circumstances:

- for reasons of national security;
- with the permission of the data subject;
- to computer bureaux (and internal audit) as part of their work;
- to prevent or detect a crime;
- for research statistics – no names mentioned;
- for payroll and accountancy purposes;
- when required by law or by court order;
- to prevent damage or injury to a person.

There are several offences under the Act:

1. giving false or misleading information
2. obstructing a person who has a warrant for entry and inspection
3. not complying with an enforcement notice
4. not maintaining a current register address
5. contravening registration requirements.

The enforcement process goes through degrees of severity, per Figure 7.29.

Are You Protecting Your Digital Assets?

By Dan Swanson, Compliance Week Columnist

Safeguarding assets has been an important objective of all organizations for centuries. In today's digital age however, what does safeguarding your assets really mean? Who is responsible for it? And how is "protection" actually achieved. The COSO framework for enterprise risk management recognized the importance of safeguarding assets as an implicit component of effective internal control. Its landmark 1992 framework even defined internal control as: "[A] process … designed to provide reasonable assurance regarding the achievement of objectives

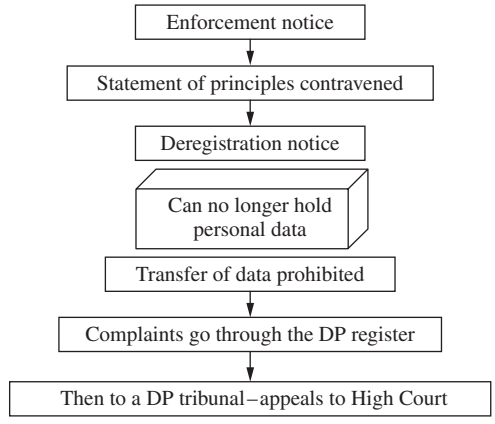


FIGURE 7.29 DP enforcement process.

in the following categories: effectiveness and efficiency of operations; reliability of financial reporting; and compliance with applicable laws and regulations.''

You can't provide reasonable assurance of your operations or financial reporting unless you know what your assets are, where they are, and who is doing what with them. You need to know your assets are protected. Before 2000, protecting an organization's assets consisted mainly of physical safeguards, asset management (for example, taking inventory of your goods), and monitoring asset values. Although these practices are still critical in today's business environment, additional processes, procedures, and controls are required to protect our information assets. With a high percentage of market value now accounted for by intangible assets such as intellectual property, reputation, brand, and electronic records, information is now a vital business resource. And, as with physical assets in earlier post-industrial times, the vulnerability of today's valuable informational assets to theft or other criminal attack has made protection of such assets a matter of immense urgency for all organizations.

Who is Responsible for Information Asset Protection?

While chief information security officers and chief financial officers are important players regarding information asset protection and security, they are not the true ''guardians'' of the organization's critical informational assets. For example, in hospitals, CFOs are not responsible for safeguarding patient records; at insurance companies, they are not the guardians of policyholder records. In the pharmaceutical or technology sectors, the company's crown jewels (its intellectual property) are not the direct responsibility of the CFO or the CISO.

All of these forms of data have associated expenses and are used to generate revenues (billings, annual fees, royalties), for which the CISO has ultimate security oversight. The CISO in turn must ensure the integrity of the chain of custody by enforcing rules applicable to key managers and other authorized personnel in their roles as the day-to-day ''guardians.'' In short, internal control is affected by people at every level of an organization. In fact, many managers are more directly responsible for day-to-day asset protection than the CISO or CFO.

What Are the Implications?

Addressing these questions will help determine key implications of how to protect your digital assets and what actions to take.

- Will an organization's information security management system become critical to the safeguarding of the CFO's financial records? Will those systems emerge as the key means of safeguarding an organization's assets?
- Will CFOs and finance staff need to understand and implement informational asset protection measures to be effective in their roles of supporting the guardians of the organization's assets?
- Will we need more guidance on the definition, classification, and protection of information assets?
- Will CISOs need to work more closely with and educate the finance function (and all operating departments, really) about how to best implement a sustainable information protection and security program?
- Should the organization establish a data management function and data governance policy, standards, and procedures? Both the function and governance could be the headed by a senior manager reporting to the chief operating officer or chief executive officer. What role(s) could the chief information officer take in information protection?
- Will the Board and CEO need to provide more in the way of expectations?
- Will internal audit and external audit spend more resources on evaluating the protection of all of an organization's assets, physical and digital?
- The internal audit function in particular needs to think more strategically about enterprise-wide security and ensure that enterprise-wide risk management is a guiding theme for prioritizing the organization's efforts.

The Big Question: What Should We Do?

First, top management must convene a council of chief-level executives including the CEO, CFO, CIO, CISO, CAE (chief audit executive), and other chiefs including compliance, risk management, and all areas of the business that own, maintain, use, or rely upon information. The most senior members of this council must ensure all members understand the critical reliance on information security and the financial, regulatory, social, and other impacts that can befall the organization if information security is breached. This understanding must be expressed in non-technical business terms to ensure everyone competently understands the level(s) of risk the organization can and cannot accept with regard to protecting information assets. Only with this comprehensive level of understanding can management ensure resources dedicated to information security are in line with the criticality of protection required by the organization.

As a next step, this C-level council must collectively ensure the security resources and solutions in place are appropriate to manage the business risks within the bounds of external requirements and the business appetite for risks. And security monitoring must ensure the appropriate level of protection will remain in place and functioning. The bottom-line: Top management must implement an information

security management program that truly safeguards all assets of the organization. Organizations that have not done so already should immediately:

- Discuss information security with the board and senior management, ensuring their understanding of the key risks and gaining their support for the necessary controls;
- Link security investments and resourcing to core business priorities and risk-assessment results;
- Leverage existing security standards, guidance, and practices and define the organization's information security management system;
- Explicitly assign responsibility and accountability for protecting informational assets across the organization;
- Revisit IT and related strategies to align business and IT efforts, and ensure that overarching information security requirements are explicitly defined;
- Inventory and classify the organization's information: Identify it, assign a business guardian to it, and determine how best to protect it based on risk-assessment results;
- Implement common security practices and solutions to meet business needs and comply with ever expanding regulatory compliance requirements;
- Identify continuous improvement opportunities and prioritize them, and then invest in improving the operational resilience of the organization;
- Strengthen the business continuity program;
- Configure security into both business processes and the supporting IT systems, to strengthen technical and procedural security practices;
- Include ''Asset Protection in the Digital Age'' as one of the discussion items in quarterly business performance review meetings, and develop action plans for improvement as needed.

We must build security into and across all organizational efforts. The CISO and CFO each have a mandate to work with the other key corporate players – and especially the business guardians of informational assets – to ensure effective asset protection. This is definitely a responsibility shared by various players throughout the organization. The question is, do the players work together to ensure effective asset protection? Or do they work on this critical responsibility in silos, allowing things to fall between the cracks? Are we also addressing information protection in all the outsourced activities that are so prevalent today?

Leaders also need to ensure that all vendors, suppliers, and other third parties responsible for protecting information used in outsourced activities are included in the mix of information asset protection and security actions.

As a colleague recently indicated, we need to move away from financial, operational, and technological thinking and decisions toward a critical-thinking methodology meant to maximize the benefit to the enterprise as a whole, not sub-units of it. That is based on enterprise-wide risk assessment and management. Are all your organization's assets appropriately protected in the digital age? I recommend making this a topic of discussion at your next management committee meeting, or better yet, put it on the board agenda. An effective tone at the top starts with top management and the board taking action to implement appropriate security controls.

Reprinted from *Compliance Week*. This article was originally published in Compliance Week. Reproduced by permission of Compliance Week. All rights reserved.

Computer-assisted Audit Techniques (CAATs)

Internal auditors are charged with securing sufficient evidence to support their audit findings and to be of any use, this evidence must be reliable. Auditors need to test automated controls and select and test transactions held on computer files. To extract the necessary evidence and meet these two objectives it is necessary for the auditor to get inside the system (i.e. the computer) and secure all automated data. This occurs during testing routines where controls are being tested either for compliance or for effectiveness. Because of the auditors' special position in the organization and the need to assume a level of independence, it is inadvisable to rely on management to provide all the required evidence. It should ideally be extracted by the auditor, and the fact that it may be held on magnetic media should not affect this. The auditor must then use automated facilities to assist the audit of computerized operations and these are the CAATs. The process for applying audit interrogation packages is illustrated in Figure 7.30.

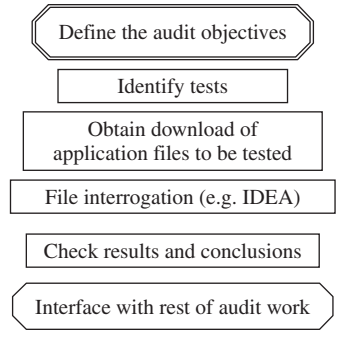


FIGURE 7.30 Computer interrogation process.

Internal audit should ensure that they have full access to all organizational systems and that this access is available from within their offices. Downloading is another facility that should be available where relevant data is secured by the auditor for importation into a suitable interrogation package. Automated data should be subject to audit testing just as other sources of information are. The link between test data and enquiry facilities may be illustrated as in Figure 7.31.

CAATs must be used to achieve a control objective and this tends to be applicable to the various testing routines that the auditor may have designed. We should never construct or acquire a set of sophisticated techniques looking for suitable problems to solve. In selecting the most appropriate technique to use the auditor may consider a number of factors:

- the level of assurance that the auditor requires;
- the level of technical expertise available to the audit department;
- the importance of the system;
- whether the review is one-off or a continuing matter;
- the set-up time and cost;
- the adopted audit approach;
- the level of independence required;
- the time and cost of maintaining the technique;
- the complexity of the audit test.

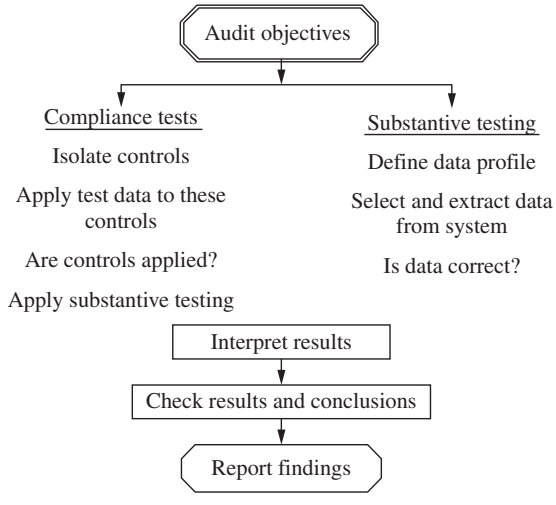


FIGURE 7.31 Audit testing.

Interrogation software, as the name suggests, may be used to analyse downloaded data from computer files. This is important when applying walk-through tests, compliance tests and substantive tests. Where a package such as IDEA is applied the computer auditor may:

1. select transactions from a file as a download;
2. extract exceptions for special attention – we may look for oddities, items outside a defined range, duplications, items missing from a number sequence, irregularities, invalid fields and so on;
3. make an analysis of frequencies and patterns with a view to isolating areas of concern;
4. stratify data;
5. validate data;
6. recreate audit trails;
7. highlight items not conforming to systems rules, not sensible, of audit interest, or duplicated processing;
8. use this to confirm that the system is not working, the input is wrong or that the processing is wrong.

This is useful with high volumes of data, lack of an audit trail, computer-generated transactions, lack of printouts, or a paperless environment. The auditor may question whether management should have access to and be using such specially generated information and this may become an audit finding. Test data may be used to recreate the type of transactions that the system will process and so test the correct functioning of systems controls. Points to note regarding the use of test data:

- to test processing logic;
- to test correct operation of controls;
- to test algorithms in programs;

- need not rely on the normal production run;
- can only test preconceived controls that are documented.

There are alternative ways that test data may be applied:

1. **Live processing/live data.** Data that conform to the test requirements will have to be found by sifting the input data.
2. **Dummy data/live processing.** A higher level of assurance will be needed to negate corruption by manual adjustments and journals. This should be discussed with the IS manager beforehand.
3. **Dummy data/dummy processing.** This may cover all features of data. It is run against copies of files and programs and so does not disrupt processing. The dummy programs may, however, become out of date and so need to be maintained.
4. **Test data generator.** This creates large volumes of test data through the utility software.

Computer-generated evidence may be used in court if certain rules are complied with:

Civil cases

- The information is derived from data supplied to the computer.
- The computer is working properly and is regularly used for the purpose.
- Data are regularly provided.
- The evidence must be legally admissible.

Criminal cases

- There are no grounds for the computer being inaccurate and any errors in the computer do not affect data.
- A certificate signed by the responsible officer is required, which identifies the data and the computer.
- The evidence complies with relevant law.

Application Auditing

The IS strategy, IS security and methodology through which new and enhanced systems are developed and brought online all contribute to the control environment for information systems. This environment ensures that applications such as stores, income, payments, business processes, performance management, financial accounting, budgeting, ordering, planning systems and so on are applied in a controlled manner. Information systems will have the basic components of inputs, processing and outputs as data are translated into information, which then supports decision-making. It is possible to audit applications by considering some of the standard controls over inputs, process and outputs and a list of such controls can be used to ensure information is complete, reliable, authorized and properly processed and stored. Note that the best way of developing controls is to perform an assessment of risks and build the control solutions around a clear risk management strategy that addresses the more significant risks. A list of possible application controls follows:

There are several basic input controls:

User procedures
Disciplinary hearing with instant removal of staff
Physical access restrictions
Encryption
Double keying and verification
Completeness, e.g. batch numbers
Well-designed input documents
Validation (display data after routine)
Access, security and passwords control
Control totals
e-transfers authorized
Controlled stationery
Validation – range, format, reasonableness
Staff training and recruitment
Segregation of duties
Firewalls and authentication routines
Anti-virus software
Authorization
Batch control (where appropriate)
Turnaround documents
Accuracy checks
Call back for remote access
Sequential numbers
Supervisors review and authorization
Error messages

Processing controls are set within the underlying application software and include:

- overflow flags that indicate where excess digits have been used;
- range checks – so that a transaction must be between, say, £0 and £20,000;
- validity checks – say, checking that a correct code has been used;
- format checks – ensure the item is either alpha or numeric;
- compatibility checks – ensuring that a consistent field is used;
- exception checks – for example, overtime only given to certain grades of officers;
- systems failure controls;
- file identification controls;
- run-to-run controls – for example, total gross pay from the Gross Pay program should be the input to the Net Pay program;
- duplicate input checks;
- sequence checks on consecutive numbering;
- check digits;
- completeness checks, for example, all fields covered and all data accounted for;
- the whole validation program;
- reconciliation of related fields;
- checkpointing – saving transactions at a certain point in time;
- logical routines;
- record count;
- control totals;
- missing data checks;
- limit checks;
- recovery procedure;
- exception reports.

Output controls include:

- suitable reports;
- working documents;
- reference documents;

- error reports;
- good security arrangements for reports in line with DP rules;
- manual procedures to ensure all reports reach their destination;
- screen viewing restricted to authorized personnel;
- prioritization of output;
- security over valuable stationery;
- independent check on all output;
- reports only sent to authorized users;
- mechanisms to ensure that the output is received in a timely fashion;
- the appropriate media used;
- appropriate format;
- well-planned error and exception reports;
- user feedback to ensure that reports are no longer sent where they are not used;
- completeness schedules of expected output;
- data quickly resubmitted wherever necessary;
- exceptions investigated by a responsible officer;
- all expected output received;
- an adequate transaction trail available so that data may be traced to the original or through the system;
- secure printers;
- disposal of documents and reports;
- rules on automated document retention and storage;
- exception reports;
- page numbering;
- shredders for confidential waste.

The traditional audit approach to information systems was typified by the auditor analysing reams of computer printouts. It ignores the existence of the computer and client management is relied on to provide information the auditor requires. In circumstances where audit is operating on a consultancy basis, this can be acceptable. In the normal course of business, it is necessary to preserve a level of independence and so adopt a more proactive line. The auditor must be able to stand back from management and be able to secure the information required. This may either be done through liaison with IS support or building special audit facilities into systems at development stage. Alternatively, the audit department may develop its own suite of software to extract data and test controls. IS audit then comes into its own, but if this is not being addressed, the audit function will eventually become locked out of the organization's computerized systems. The IS auditor should spend time working with other auditors on their interrogation needs and how test data will be developed and applied. The CAE should ensure that this happens and that audit policies build in this important issue.

Auditing Information Security: Are You Protected?

By Dan Swanson, Compliance Week Columnist

I recently read that many people worry about accidental death, particularly in ways that are very frightening: poisonous snakes or spiders, or even alligator attacks. This same article noted that based on official death statistics, the vast majority of people actually die from chronic health causes: heart attacks, obesity, and other ailments that result from poor attention to long-term personal fitness. In 2003, accidental deaths in the United States numbered around 100,000; chronic health-related deaths

were more than 2.4 million. The point is people must focus their attention in the correct places when they consider what would most influence the quality of their lives. Exactly the same issue exists at organizations where the board and management must ensure they build and sustain the long-term health of the organization. This concept also applies when auditing information security. Does your information security program need to go to the gym, change its diet, or perhaps both? I recommend you audit your program to find out. The internal audit department should evaluate the company's health – that is, internal auditors should evaluate the critical functions of the organization for long-term sustainability. Do risk-management efforts identify and focus on the right risks? Does senior management encourage the right level of risk taking within defined tolerances? Is the status quo challenged regularly? Is the company considered a good place to work? What could bring the organization down, and are measures in place to prevent or reduce that possibility (say, by running continuity scenarios and exercises)?

To that end, internal audit should have regular talks with management and the board regarding the organization's information security efforts. Are management and staff anticipating tomorrow's requirements? Is the organization building ''muscle'' for critical security activities (policy development, awareness and education, security monitoring, security architecture, secure code development, research and development, and so forth)? Is there a comprehensive security planning process and program? Is there a strategic vision, mission, strategic plan, or tactical plan for security that is integrated with the business? Can the security team and management sustain them as part of conducting day-to-day business? Is the information security program focused on the critical information protection needs of the organization, or is it worried about the accidents? Are the results of security efforts reported regularly?

Evaluating Security

The exact role of internal audit regarding information security varies widely among companies, but it always provides a significant opportunity for internal audit to deliver real value to the board and management. Internal auditors should play an important role in ensuring that information security efforts have a positive effect on an organization and protect the organization from harm. Why worry so much about information security? Consider some reasons why organizations need to protect their information:

- Availability. Can your organization ensure prompt access to information or systems to authorized users? Do you know if your critical information is regularly backed-up and can be easily restored?
- Integrity of data and systems. Are your board and audit committee confident they can rest assured that this information has not been altered in an unauthorized manner and that systems are free from unauthorized manipulation that could compromise reliability?
- Confidentiality of data. Can you tell your customers and employees that their nonpublic information is safe from unauthorized access, disclosure, or use? This is a significant reputational risk today!
- Accountability. If information has been compromised, can you trace actions to their source?

An audit of information security can take many forms. At its simplest, the auditors will review the information security program's plans, policies, procedures, and key new initiatives, plus hold some interviews with the key stakeholders. At its most complex, a large internal audit team will evaluate almost every aspect of the security program and even do intrusion testing. This diversity depends on the risks involved, the assurance requirements of the board and executive management, and the skills and abilities of the auditors. For example, if the organization is undergoing extensive change within its IT application portfolio or IT infrastructure, that would be a great time for a comprehensive assessment of the overall information security program (likely best just before or just after the changes). If last year's security audit was positive, perhaps a specialized audit of a particular activity or an important e-commerce application would be useful. The audit evaluation can, and most times should, be part of a long-term (read: multi-year) audit assessment of security results.

Defining the audit goals, objectives, and scope for a review of information security is a vital first step. The organization's information security program and its various measures cover a broad span of roles, processes, and technologies, and just as importantly, support the business in numerous ways; security really is the cardiovascular system of an organization and must be working at all times. Firewalls, monitoring technologies, encryption software, network architectural design, desktop asset management, identity management solutions, high-availability solutions, change management and change auditing systems, logical access control solutions – the list of security systems, technologies, and processes used is almost endless. The planning phase of the audit needs to ensure the proper focus and depth of audit evaluation. Internal auditors need to determine the level of their involvement, the best audit approach to take during the audit planning, and the skill sets they'll need.

The decision about how aggressively internal auditing should evaluate information security should be based on an audit risk assessment and include factors such as risk to the business of a security compromise of a critical asset (information or system), the experience of the information security management team, size and complexity of the organization and the information security program itself, and the level of change in the business and in the information security program. Information security standards dictate that information security controls should be selected in the light of an asset-level risk assessment. Aggregating assets is sensible when one is dealing with a group of like assets exposed to the same risks (''risk'' being defined as the likelihood of an identifiable threat exploiting a specific vulnerability). Auditing information security should, therefore, include auditing the organization's risk assessment process and the appropriateness of the controls selected, implemented, monitored, reviewed, and updated as a result of the risk assessment.

Moving To Continuous Improvement

Like most audits, audit of an information security program will generally involve three phases: planning, fieldwork, and reporting. Information security programs, however, come in many shapes and sizes, so the audit of information security must be flexible and risk-based. The audit should encourage the organization to build strength, endurance, and agility in its security program efforts. During the planning phase, the internal audit team should ensure that all key issues are considered, that the audit

objectives will meet the organization's assurance needs, that the scope of work is consistent with the level of resources available and committed, that coordination and planning with IT and the information security staff has been effective, and that the program of work is well understood by everyone involved. It is important that the audit scope be defined using a risk-based approach to ensure that priority is given to the more critical areas. Less-critical aspects of information security can be reviewed in separate audits at a later date. In the fieldwork phase, the auditor analyzes the various components of the information security program based on the scope identified in the planning phase. Among some of the important questions that may be asked in a typical audit are:

- Does the information security program reflect the risks and complexity of the organization?
- Is the program actively investigating and implementing new ways of protecting the organization from harm based on threat trends?
- Is there an active education and awareness effort, so that management and staff understand their individual roles and responsibilities?
- Are the security measures and controls regularly tested for operational effectiveness, and are corrective actions occurring?
- Is performance being measured and reported to stakeholders?
- How does the organization's security compare with other well-run similar organizations?

Audit tests could include reviewing program plans and budgets, interviewing key executives, looking at security training material, reviewing management test plans to evaluate operating effectiveness of security efforts and their results, reviewing management's communications to employees regarding the importance of security to the organization and how it contributes to long-term success, and studying the support and trends for performance reporting. On the more technical side, try assessing intrusion detection practices; testing of physical and logical access controls; and using specialized tools to test security mechanisms and potential exposures. The evaluation of business continuity and disaster recovery efforts could be considered as well.

The bottom line is that internal auditors should be the company doctor: (1) completing regular physicals that assess the health of the organization's vital organs and verifying that the business takes the necessary steps to stay healthy and secure, and (2) encouraging management and the board to invest in information security practices that contribute to sustainable performance and ensuring the reliable protection of the organization's critical assets.

Reprinted from *Compliance Week*. This article was originally published in Compliance Week. Reproduced by permission of Compliance Week. All rights reserved.

7.7 Compliance

The IIA Attribute Standard 1220.A1 deals with due professional care and says that internal auditors need to consider the:

- Extent of work needed to achieve the engagement's objectives;

- Relative complexity, materiality, or significance of matters to which assurance procedures are applied;
- Adequacy and effectiveness of governance, risk management, and control processes;
- Probability of significant errors, fraud, or noncompliance; and
- Cost of assurance in relation to potential benefits.

We have indicated before that IIA Performance Standard 2120.A1 says that the internal audit activity must evaluate risk exposures relating to the organization's governance, operations and information systems regarding the:

- Reliability and integrity of financial and operational information.
- Effectiveness and efficiency of operations.
- Safeguarding of assets.
- Compliance with laws, regulations, and contracts.

Compliance is an issue for the internal auditor and during the audit, an assessment will be made of the extent to which the business is adhering to laws, regulations and control standards. The Performance Standard 2210.A3 confirms that:

> Internal auditors should review operations and programs to ascertain the extent to which results are consistent with established goals and objectives to determine whether operations and programs are being implemented or performed as intended.

While compliance and issues relating to regularity and probity are generally incidental to the main audit objective in assessing significant risk and controls, there are times when internal audit may need to launch into an investigation into specific associated problems. In many developed countries, a failure to demonstrate compliance with anti-money laundering can lead to the possible closure of the business, the seizure of assets or the revocation of operating licences. Some audit teams have compliance reviews built into their official terms of reference. For example, a review of security measures may find that remote parts of the organization may have failed to meet the corporate security standards as illustrated below:

> Police have called for an inquiry after a new age traveller was found living on a government-licensed cannabis plantation. The teenage girl had parked her rusting bus among the 12 ft high plants and was helping herself to the crop, which should have been guarded by a farmer . . . police visited the plantation after a tip-off found security measures were 'non-existent' . . . [50]

There are many banks, financial services companies, large retail outfits and other organizations that are either highly regulated or consist of hundreds of branded branches using the same basic operational and financial systems. The main worry from the board is that parts of the organizations are out of step with requirements and the internal audit team is charged with carrying out compliance reviews as a main way of tackling this high-level risk. Automated data analysis enables such audit teams to target high-risk areas of those with possible problems of non-adherence. However, the value-added proposition is that compliance reviews are the main thrust of the internal audit work.

In terms of the ongoing review of compliance with laid down procedures in those high-risk sectors such as banking, financial services and retail, regular testing and visits to local establishments are a main feature of audit work. Management must establish operational procedures and suitable standards of financial management for all operations, particularly for remote locations and

decentralized activities. They must also check on the extent to which these standards are being applied. A formal programme of probity visits may be commissioned and effected possibly on a spot-check basis. Internal audit would recommend management makes these visits as part of the systems of control over these decentralized operations. It is not necessarily the primary role of internal audit to carry out these probity checks. It may be that the audit function is required to operate a series of compliance checks as part of their role in the organization. A formal terms of reference and budget for the work will be required and this should be set out and agreed on with management. Probity audits should be carried out via an agreed programme of visits that may be scheduled well in advance. The term 'programme' may also refer to a schedule that records the tasks that should be completed during the audit, which should be drafted by the audit manager. Standard programmes may be applied, but they should be tailored to the actual probity audit that is being performed and, as such, it is good practice to hold a set of these programmes in the audit library. A procedure for carrying out probity audits is as follows:

1. The work will be agreed on with senior management and this may involve a one-off visit or a series of programmed visits.
2. The appropriate line manager should be contacted and a date set for the visit. It is possible to distribute an audit information brochure in advance of this visit.
3. It is possible to apply standardized documentation to this programmed audit work. Probity visits should not be allowed to consume excessive audit resources and the approach will be to apply junior staff wherever possible and work to tight budgets of up to, say, a week. This will depend on the type of audit.
4. Visits to remote establishments/operations should include:
   - a cash-up;
   - vouching a sample of transactions from the banking arrangements;
   - inventory checks covering all valuable and moveable items;
   - a check on a sample of local purchases and tests for compliance, integrity and effect on the cost centre;
   - a programme of tests applied to all areas that may be vulnerable to fraud or irregularity;
   - verification of a sample of returns made to head office;
   - other checks as required or agreed with management.
5. The work undertaken will have to meet the standards set out in the audit manual and any appropriate documentation and report format should be agreed on with the audit manager.
6. The standards of review should comply with the audit manual, and supervisory review and performance appraisal documents should be used by audit management.

Where it is not possible to resource probity audits, the alternative approach will be to advise management on how best the work might be organized. This may include assisting in the process of drafting the relevant probity audit programmes along with providing management with support and training. Management is charged not only with establishing suitable procedures for controlling their resources, but also with ensuring that these procedures are complied with. We have argued that as part of the audit consultancy role it is possible to undertake checks on compliance on behalf of management and this should follow the same procedures outlined above. Having said this, there are many companies where compliance audit is the norm and one company describes its audit work as: 'compliance audits of each branch twice a year. Check company procedures and regulatory compliance for gaming industry on fraud and money laundering. Computer-based work with lots of prep makes the visits shorter and more efficient. Tried CSA but did not work due to operational reasons.' There are additional points for compliance-based work:

1. Areas may range from health and safety, data protection, security arrangements, financial regulations, operational procedures, budgetary control, employee protection legislation, equal opportunities through to high-level policy statements. The auditor needs a clear understanding of the compliance requirements and the basis in legislation.
2. The areas most affected by the requirement to comply should be identified and listed.
3. Management compliance checks should be ascertained and evaluated for adequacy and effectiveness.
4. A programme of tests should be formulated and agreed on with the audit manager and the client.
5. The test programme should be to the professional standards set out throughout the manual.
6. The same standards of documentation and review should be applied to compliance testing.

There is a growing mass of rules and regulations that need to be observed by a corporate body and an example of some of these includes the following:

- Employment Rights (Dispute Resolution) Act 1998
- Human Rights Act 1998 – right to life, prohibition of torture, prohibition of slavery and forced labour, the right to liberty and security, the right to a fair trial, no punishment without lawful authority, the right to respect for family and private life, freedom of thought, conscience and religion, freedom of expression, freedom of association and assembly, the right to marry, prohibition of discrimination, protection of property, a right to education, the right to free elections
- National Minimum Wage Act 1998
- Public Interest Disclosure Act 1998
- Working Time Regulations 1998
- Data Protection Act 1998
- Disability Rights Commission Act 1999
- Employment Relations Act 1999
- The Equal Opportunities (Employment Legislation) (Territorial Limits) Regulations 1999
- Collective Redundancies and Transfer of Undertakings (Protection of Employment) (Amendment) Regulations 1999
- Transnational Information and Consultation of Employees Regulations 1999
- Maternity and Parental Leave etc. Regulations 1999
- Welfare Reform and Pension Act 1999
- Race Relations (Amendment) Act 2000
- Telecommunications (Lawful Business Practice) (Inception of Communications) Regulations 2000
- Part-time Workers (Prevention of Less Favourable Treatment) Regulations 2000
- Sex Discrimination (Indirect Discrimination and Burden of Proof) Regulations 2001
- Employment Tribunals (Constitution and Rules of Procedure) Regulations 200151.

One final word of warning of the dangers of an excessive focus on compliance comes from *Fad Surfing in the Boardroom* by Elaine C. Shapiro who defines non-compliance as 'My decision not to make the decisions you wish me to make the way you wish me to make them, leading to the old axiom that you can write a script to order, but you can't make me think.'[52]

Auditing Ethics And Compliance Programs

By Dan Swanson, Compliance Week Columnist

Broadly understood, compliance is an important mechanism that helps make governance effective. Monitoring and maintaining compliance is not just to keep the

regulators happy; compliance with regulatory requirements and the organization's own policies is a critical component of effective risk management. It is one of the most important ways an organization achieves its business goals, maintains its ethical health, supports its long-term prosperity, and preserves and promotes its values. An effective compliance and ethics program is best organized as integrated processes, assigned to designated business functions and managed by individuals who have overall responsibility and accountability. Compliance can be a daunting challenge, but it is also an opportunity to establish and promote operational effectiveness throughout the entire organization.

The board and management periodically need to evaluate the design and operating effectiveness of the company's compliance and ethics program. Such evaluations supplement the ongoing, day-to-day monitoring of responses and control activities. Not only do these reviews – audits, really – provide for a more in-depth analysis of the program's design and effectiveness; they also provide an opportunity to consider new practices and technologies that may have been developed since the program was first implemented.

Determining Key Risks

Defining objectives of that internal audit is the first and one of the most critical steps in setting the audit direction, because it defines the level of assurance the board and management will be provided. From the start, then, internal audit staff should hold discussions with management and the board (or the audit committee and legal counsel, as necessary) regarding the assurance needs of the key stakeholders to ensure the audit meets the assurance needs of the organization – and it should all be done prior to finishing the audit plan. Compliance and ethics programs cover a very broad span of activities, and the planning phase needs to ensure the proper focus of the audit efforts. The audit should be based on a comprehensive audit risk assessment – that is, auditors must determine what the key risks of the company's compliance and ethics program are. The participation of legal counsel in the audit is another critical factor that should be decided here, during the audit planning (or subsequently if the plan's assumptions turn out to differ from the actual audit situation). If wrongdoing is identified during the internal audit a dialogue with legal counsel is needed – indeed, it's often critical.

What objectives to set? Three goals should be:

- ***Application*** – To determine whether the compliance and ethics program provides reasonable assurance of compliance with organizational policies and applicable laws and regulations;
- ***Documentation*** – To determine if the program's management framework is documented, in place, and appropriately resourced to meet the organization's needs;
- ***Implementation*** – To determine whether the program has been implemented effectively, and that its performance reporting system has been defined and accurately presents the results of the program's efforts.

Some key issues to explore during the audit include ensuring that there is:

- ***Universality*** – Consistency and integration of compliance and ethics programs among different business units within the organization;
- ***Integration*** – Coordination between the central compliance and ethics office and individual business units;
- ***Accountability*** – A clear and effective division of roles and responsibilities among the ethics office, compliance, HR, legal, and other relevant units.

Down To Business

Any internal audit has three phases: planning, fieldwork and reporting. Audits of compliance and ethics programs are no different. During the planning phase, the internal audit team should ensure that all key issues are considered, that the audit objectives will meet the organization's assurance needs, and that the compliance and ethics program is well understood. It is extremely important that the audit focus on evaluating the significant components of a compliance and ethics program; that is, auditors should use a risk-based approach to find the program's elements most likely to fail and in most need of attention. The planning phase is an opportunity to confirm that the audit scope is appropriate, and the cost won't give anyone heartburn.

In the fieldwork phase, the team analyzes the compliance program's various components, based on the goals and methodologies identified in the planning phase. Among some of the most important questions to answer are how the board sets its ''tone at the top;'' how it communicates those values to employees; how employees at all levels of the company perceive management's commitment to those values; and how the company handles compliance or ethics issues that arise from compliance failures. Audit tests could include reviewing employee files for signed Code of Conduct or training confirmations, looking at training materials and training program results, reviewing responses to violations, conducting surveys and reviewing the results of them, reviewing management's communications to employees for ethical content, quantifying the organizational resources available for program operation, and assessing the quality of the support for the program's performance reporting. The reporting phase is where the internal audit the team should ensure all stakeholders are properly informed of the audit results and any management plans to improve the compliance and ethics program. A well-planned and executed internal audit (phase 1 and 2) should make audit reporting straight forward: tell them what you did, what you found, and what management plans to do about it. That's all there is to it.

Internal auditors must take a risk-based approach while planning a compliance and ethics program audit. With limited resources, auditors simply have no choice but to focus on the highest-risk areas and always strive to add value to the organization. Audit best practices suggest internal auditors should be involved throughout the program's life cycle, not just in post-implementation program evaluations. The internal audit of a compliance and ethics program also needs to be part of a larger overall audit plan. Internal auditors should craft a plan that meets the long-term assurance requirements of the board and management. A series of internal audits to manage complexity (if deemed appropriate during the planning phase) might not be a bad move, since a compliance and ethics program can be very information-intensive.

Management should not be developing processes, procedures, reports, and so forth during the audit. Rather, the audit team should be evaluating the efforts of the compliance and ethics program in meeting the organization's needs. Finally, management should complete a self assessment prior to an internal audit, and study various pieces of guidance such as the OCEG guide for the audit of a compliance and ethics program.

Reprinted from *Compliance Week*. This article was originally published in Compliance Week. Reproduced by permission of Compliance Week. All rights reserved.

7.8 VFM, Social and Financial Audits

Value for Money

Part of the scope of internal audit involves evaluating the adequacy and effectiveness of arrangements for securing value for money. These arrangements consist of controls that should be established by management to ensure that their objectives will be met, and is based on promoting the managerial control system. These arrangements should involve management in a continual search for efficiencies that may result in a level of savings. It is not internal audit's responsibilities to identify these savings, and our performance measures should not include the amount of money saved through implementing audit recommendations. This point must be understood and may be restated in that we would expect our audit recommendations to place management in a position to identify areas where they may make savings. An example would be recommending that better information systems are installed. As part of our testing procedures we may be able to estimate any resultant savings, but this is not the primary role of the audit. Our duty is to get management to implement improvements in systems of control where required. It is possible to resource as part of our consultancy services VFM reviews that are designed to lead to savings for management. The Office of the Auditor General of Canada says about VFM:

> A VFM audit is a systematic, purposeful, organized and objective examination of government activities. It provides Parliament with an assessment on the performance of these activities; with information, observations and recommendations designed to promote answerable, honest and productive government and encourages accountability and best practice. Its scope includes the examination of economy, efficiency, cost effectiveness; accountability relationships; protection of public assets; and compliance with authorities. The subject of the audit can be a government entity or activity (business line), a sectoral activity, or a government-wide functional area.[53]

There are two views of VFM: VFM in its true sense is about the way management organizes and controls its resources to maximum effect. The narrow view sees VFM as ad hoc initiatives that result in defined savings and/or a greater level of service/output. VFM results in:

- **Economy.** Resources required to perform the operation are acquired in the most cost-effective manner.
- **Efficiency.** Resources are employed to maximize the resulting level of output.
- **Effectiveness.** Final output represents the product that the operation was set up to produce.

This may be represented as in Figure 7.32.

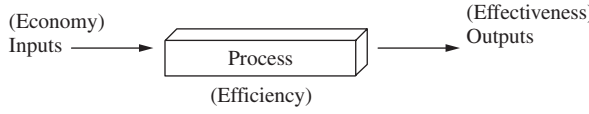


FIGURE 7.32 Value for money.

Efficiency reviews A systems-based approach to an efficiency review would consider the standards, plans, direction and type of information that management applies to controlling their operations. The investigative approach, on the other hand, concentrates on specific methods by which efficiency may be improved. This may be by applying best practice in terms of alternative operational practices, or by isolating specific instances of waste and inefficiency that may be corrected. Economy (i.e. securing the cheapest inputs) is incorporated into the wider concept of efficiency because of the intimate link between these two. Efficiency covers basic matters of economy.

Effectiveness reviews Effectiveness reviews are difficult to carry out and a systems-based approach would look to the application of sound managerial practices. This is the only way of guaranteeing that operational objectives may be achieved. Investigations into operational effectiveness (unlike systems reviews) determine whether objectives are being achieved. This requires an ongoing process:

1. defining the end product;
2. examining the current output;
3. determining whether this output is acceptable;
4. quantifying any shortfall.

Many of these matters involve an element of subjectivity and the auditor may be called upon to make what may be regarded as an expert opinion. There are many potential pitfalls and these should be borne in mind when embarking on the assignment. The concept of effectiveness must include a review of the customer's perceptions as recipients of the relevant services. A useful technique is to administer a client survey using a specially formulated questionnaire. This should be based on securing an idea of whether the services are having the desired effect on the final user. We wish to see suitable underlying systems in place to ensure effectiveness. Most of these are based on direction and good management practices underpinned by comprehensive communications systems. Effectiveness depends on setting clear objectives and ensuring these are resourced and properly communicated. While as auditors we cannot question the validity of the objectives or associated policy framework, we can review the extent to which they are supported by suitable managerial mechanisms. This encompasses the complex maze of underlying systems that must be in place for objectives to be translated into business activities.

VFM programme Some revenue budgets are compiled on the basis that a programme of VFM reviews will result in defined savings in the budget. The consultancy arm of internal audit may provide some support for this programme, and individual VFM reviews may be taken from an

organization-wide framework. We must take care not to lock internal audit into a fabricated series of target savings, where we become responsible for embarking on a search for never-ending savings to justify our existence. The system's view, where management is charged with installing suitable controls to enable them to be efficient, must be widely publicized. We would not recommend that internal audit resources become responsible for a defined VFM programme, unless unavoidable.

Accountability One interesting aspect of business life is the need to instill a degree of accountability throughout the organization starting from the top. Many operational reviews are based around the decision-making process where officials are required to formulate and apply their professional judgement and then be accountable for their actions. The empowerment initiative seeks to apply this concept at all levels of management and staff. Accountability systems must take into account competing factors:

- departmental relationships and the political implications thereof
- a clear purpose and direction
- performance review mechanisms
- full responsibilities for the activities of one's staff
- strategies and the results thereof
- suitable reporting mechanisms
- responsibility for the results of the relevant business unit
- an awareness of staff motivations and the impact on performance.

Operations profile As part of the background stage of an operational review the auditor should look at performance measures used by management to identify areas of potential waste. Much material may be gathered where the auditor compiles his/her own performance indicators (PIs) and thereby isolates potential poor performance. This may be carried out by:

- comparing similar operations;
- comparing one operation over defined time periods;
- considering variances between planned performance and the actual results.

This process may identify 'suppositions', that is, those areas where one may find a failure to secure good VFM. The auditor must weigh up the costs of preparing the PI information, and the benefits that may accrue from their use. There are many areas where operational review may impact on performance and VFM. One such list includes key areas:

Energy	Cash flow
Asset management	Transport costs
Staff numbers	Stock control
Central purchasing	Revenue contracts
Insurance policies	Support services
Duplicated functions	Centralized versus decentralized service models
Workforce planning	Temporary staff
Catering	Pensions
Overtime	Administrative costs

Reviews were in the past sensitive with the potential for organizations to shed staff as part of business reorganization. Management expects recommendations to include reductions in staff budgets. There are core areas that feature in an operational review including:

Corporate structure	Management style
Information systems	Communications
Authorization procedures	Segregation of duties
Health and safety	Supervision
Improvements	Performance review
Resource utilization	Operational quality standards
Objective setting	Compliance checks
Procedures manuals	Security arrangements
Decision-making process	Motivation
Culture	Personnel policies
Policy framework	

The Value Of 'Performance Measurement'

By Dan Swanson, Compliance Week Columnist

Steven Covey, author of The Seven Habits of Highly Effective People, and many others quite rightly recommend that when you start any kind of new project, you should begin with the end in mind. What does that involve?

1. Deciding where you want to be in the future (that is, what your ''end state'' will be);
2. Defining your key goals and objectives in getting there (to guide your various efforts along the way); and
3. Building and then implementing your plan to get there (the means to reach your desired end state).

This planning cycle works for all individuals, in both their professional and personal lives. It is even more important for organizations, where an understanding across the whole enterprise is vital in obtaining broad support across a workforce faced with numerous, and many times conflicting, priorities. For internal auditors this planning cycle takes on a special meaning as well. Successful auditing requires an understanding of what the organization is trying to achieve and factoring that understanding into the company's auditing efforts. And as an important activity itself, internal audit needs to define what the audit team is trying to achieve; without doing that, the auditing team may end up going down a wrong road during its project. For the organization to understand what the audit team is trying to achieve, the audit team itself must understand and communicate what it wants to accomplish.

The bottom line is that the auditors should be: (1) encouraging and verifying that organizations have robust systems to measure and report performance; (2) be leveraging the information from such systems in planning their audit efforts, and finally (3) walk the line themselves, by defining their long-term goals, the means to get there, and reporting their progress to the audit committee.

Where Performance Management Fits In

As part of tracking the audit's progress, periodic measurement and reporting is vital, and serves as a bridge between today's work and tomorrow's. Put another way, an audit team must define its road map, get agreement with all the stakeholders that the

path is correct (including the auditing project's goals, the plan, and proposed end-state), and then monitor and report progress in getting there. A robust performance measurement and reporting program facilitates the ongoing monitoring of progress, the regular (and sometimes painful) debate of issues and interim results along the way, and the corrective actions and adjustments necessary to remain headed where you need to go.

All of the above concepts apply at the various levels of the organization, from the enterprise as a whole down to subsidiaries and significant business units. As the internal auditing team evaluates various aspects of the organization, each audit should consider in its evaluation whether performance measurement and reporting is contributing to the setting of direction and the execution of plans.

The Art Of Measurement

A well-known maxim is, ''What gets measured gets done.'' All enterprise processes, including an audit, can benefit from measurement. Ideally, measurement will help an organization:

- show how these results support organizational objectives;
- determine what works and what doesn't;
- justify capital allocation;
- motivate and provide tangible feedback to employees; and
- enhance the ability to communicate with stakeholders.

A critical element of performance measurement is establishing key performance indicators and metrics. In thinking about metrics, they need to be ''SMART'' – that is, Specific, Measurable, Actionable, Relevant, and Timely. Another important consideration is not to overload the process with too many metrics but to focus on those most relevant to assuring the organization is creating shareholder value. (One excellent reference guide is the Open Compliance and Ethics Group's metrics and measurements guidance.)

For auditing and compliance efforts, performance measurement and reporting allows auditing and compliance professionals to work with their clients (and fellow employees) and other stakeholders to define the goals, the roadmap, and the end-state the organization is working toward. What ideal system of operation does the company want to have? What should be tested to see whether the company is achieving that goal? What should be improved? How can you measure performance to gauge how well that improvement is happening? Debating ahead of time what measures will be considered for the formal performance reporting will help ensure that everyone is on the same page and that surprises can be anticipated. In addition, we always say we need to improve communications (the number-one cause of failure, by far, in most everything we do). Defining your performance measurement and reporting program is a vehicle to have discussions on what's important, what your priorities are, and where you want to go. Knowing that makes an auditing project enormously easier. Performance measurement and reporting on organizational and auditing efforts offers a strategic opportunity for the compliance and the internal audit departments to influence the entire organization's governance efforts. Consider taking it on!

As mentioned, internal audit should weigh incorporating an evaluation of performance measurement and reporting into each audit performed. Auditing the organization-wide performance measurement and reporting program is also strongly recommended. An audit will provide for an independent and objective review of the efforts of the organization to define its goals and objectives, take action on them, and monitor progress, including corrective actions as things happen (and they will happen). Evaluating the program involves defining the system to be audited; assessing the measures being used, the processes in place, and the operating effectiveness; and determining whether improvement to the system will have an effect on the organization's results.

Improving the organization's operational performance is always a critical priority, and implementing (or enhancing) a formal performance measurement and reporting program will help greatly. It ensures that the organization stays on track with its overall objectives, and failing to audit that control creates a significant gap in the overall audit coverage.

Reprinted from *Compliance Week*. This article was originally published in Compliance Week. Reproduced by permission of Compliance Week. All rights reserved.

Social Audit

The growing interest in the way business interfaces with its environment is now accepted. In the past, management has perceived the external environment in a limited way, which views outsiders as consisting mainly of:

Customers	Competitors
Government	Potential workers
Retail outlets	Potential new markets
Suppliers	

This view takes on board forces that impact on the future success of an organization in terms of its ability to meet its objectives. This may be based on profit margins or service delivery goals, depending on its role. Social and environmental auditing changes this position. Here executives are encouraged to consider the wider impact of their business on society in general, in recognition of the long-term implications of their activities. Environmental considerations have to be accounted for and audited, and the internal auditor should develop an interest in this important topic. Social auditing views the wider role of an organization, which may have to take into account many external factors including those shown in Figure 7.33.

In considering social audit, there are several issues that should be mentioned:

External image The starting place for social audit is to reassess the public image of the organization. There are now organizations that advertise their image rather than their products.

With the growing spate of takeovers and mergers, it is sometimes difficult to judge exactly what an organization produces. Product diversification and expansion of product ranges can make this factor somewhat obscure. What is more important is the reputation of the company, and this is now a guide to the buyer of its quality and worth. The audit input may start with reviewing the mechanisms that the organization has established to obtain feedback on its standing in the business world. Government entities are more susceptible to press coverage where any public scandal has a direct impact on its senior executives. We restate that audit is not primarily

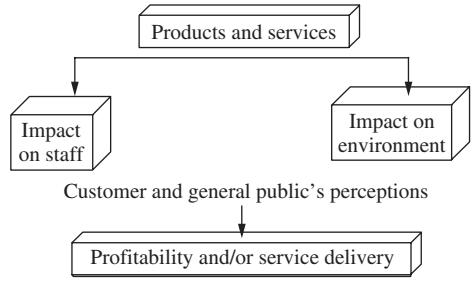


FIGURE 7.33 Social audit.

concerned with the public perception of the organization. It is more interested in the adequacy and effectiveness of systems for promoting the corporate image and receiving feedback on the current position.

Environmental auditing This is primarily about protecting the environment for future generations based on the caretaker concept. Here organizations are deemed to owe an additional responsibility to future citizens over and above all those we discussed earlier. There is now an entire range of ISO standards on environmental auditing (ISO 14010 range). This calls for effective environmental management systems and procedures that must be in place to meet the requirements of this standard. Brian Rothery has written extensively on quality assurance and environmental auditing standards and has expressed the view that accountants and auditors have missed the opportunity to become involved in implementing and auditing quality management systems, and will likewise miss out on environmental auditing if this same attitude is assumed. Management consultants and engineers, however, have quickly grasped these new opportunities.

Denial Another concern for the auditor is the current state of the organization in terms of its recognition of the wider social implications of its business activities. Where there is little or no appreciation of the value of social audit, the main thrust of the audit may be educational in nature. A review of similar organizations to gauge a comparative position may reveal the extent of this problem. Environmental auditing should be set firmly on the agenda of the board of directors and should feature in annual reports and other publications. How far the directors have reached and how far they may need to go is a worthwhile audit comment as a way into this complicated topic. Securing extensive insurance policies and engaging teams of lawyers to combat any threats of legal action for breach of external regulations, equal opportunities, industrial tribunals, fines for pollution and breach of ethical rules and extensive customer complaints indicate an uncaring attitude or uneducated management. Proactive steps to ensure these problems are contained relies on a longer term view where the organization's reputation is uppermost in the minds of management.

Implications The auditor needs to keep in mind the results of a failure to manage the environmental implication of a business. It is not about being a loving, caring organization that has a 'warm' feel. It is about generating a positive reputation that provides a clear role in society, where the rights and concerns of current and future generations are taken on board when defining corporate strategies. For example, it is very expensive to administer a 'no questions asked' policy for returned goods, although in the long term this will enable a good reputation to be claimed. Recognition of social responsibility does have a cost. It must be justified in terms of long-term implications

for the future welfare of the entity. Compiling a cost–benefit analysis is another key control over the process of developing appropriate initiatives. The difference is the time frame where social awareness takes many years to translate into an enhanced commercial position. There is a view that consumer behaviour is quite sophisticated in that it eventually responds to an organization's conduct. At the extreme, buyers may boycott goods from 'suspect' countries, 'suspect products' or for that matter entire companies. An oil exploration company that faces allegations of unfair practices or environmentally disruptive activities may experience a backlash from its customers.

The Green movement The Green movement is an established tradition that operates in many countries. It is a pressure group with political representation in many societies. This is important because it may take the initiative away from an organization. There are times when a form of coercion may appear that seeks to force a change of corporate policy outside the control of executive management. The audit role can be located in a continuum where on the one hand it reviews mechanisms that the organization has established to manage its social responsibilities. On the other hand, we may review the reaction of the organization to external forces that seek to influence business activities that are seen to damage the environment. We may start from a managerial stance and end up with a costly damage limitation response. The auditor may expect the organization to recognize the role of pressure groups in society and ensure that they are able to pre-empt adverse publicity through the implementation of suitable mechanisms. At best these systems will keep the organization ahead of the game, while at least they should represent early warning systems where adverse responses are anticipated and minimized. The auditor will want to see these considerations addressed and dealt with by executive management.

Health and safety This is an area close to home for most senior directors. The auditor may review a range of responses. A reactive response will entail a basic recognition of health and safety procedures, while a more dynamic response will entail various risk profiles for all operations and work areas. This enables management to target key areas and ensure that the health risks are properly managed. Returning to this two-dimensional view of corporate responsibility, we may encourage management simply to defend the organization by complying with health and safety regulations. Alternatively, we may wish to promote a culture where the welfare of employees is considered over and above basic compliance with laws. Much depends on where this issue is located on the corporate agenda. An organization that damages the health of employees will always be subject to criticism. An audit of health and safety will establish the presence of several key mechanisms:

1. a key officer responsible for promoting this function;
2. a committee of senior representatives from each work area;
3. health and safety firmly on the agenda at board meetings;
4. training for line managers and operatives;
5. suitable publications and signs located across the organization;
6. a policy that locates responsibility for health and safety with management;
7. a risk-based approach that seeks to isolate key potential problem areas – this is an ongoing exercise that should be undertaken by management;
8. a budget for the use of health and safety experts wherever necessary;
9. a zero-accident policy that is fully supported throughout the organization;
10. a procedure for investigating the causes of accidents, near-accidents or relevant incidents.

Corporate code of conduct and business ethics We have dealt with the need for clear standards on business ethics in Chapter 2. We also touched upon the need to install effective

mechanisms to help guard against fraud and corruption in this chapter. Again, social responsibility assumes that key corporate figures who control many millions of pounds of resources are held in the public eye. When staff are being forced to take pay cuts, then senior executives may take the lead and voluntarily forgo a pay increase or even draw a smaller salary. This responsibility extends to many areas where top management is expected to set standards. The auditor will once again review the extent to which suitable procedures are in place to ensure that high standards of conduct will ensue. It is possible to teach business ethics and establish a programme where the underlying issues are defined and assimilated into business life.

Press relationships and advertizing standards An auditor who wishes to know how far an organization values its public name needs only visit the public relations office (or press office). If this office is dynamic and anticipates the type of information that the public need, then there should be little that cannot be properly managed. The process of managing the media is part of the control system that the auditor will review. Again, we would look for a position where the organization takes the initiative on environmental issues and is not one step behind public pressures.

Equal Opportunities Legislation requires all organizations to comply with certain aspects of promoting equal opportunities. These tend to cover race, sex and disability and are designed to ensure that these groups are not disadvantaged in terms of employment opportunities. They tend to be part of 'good employment' practices rather than enforced legal requirements. As with all policies, they may be subject to an internal audit coverage in terms of the adequacy and effectiveness of controls that promote the successful implementation of the policy. These controls include suitable recruitment, selection procedures and monitoring of staff movement on organizational mechanisms such as promotion, staff discipline and training programmes.

Pollution One fundamental concern across all parts of society relates to the physical impact of an organization's processes in terms of pollution. This may include river pollution, scarring the landscape, chemical emissions, excavation work, dumped rubbish and so on. The audit review will assess the extent to which an organization may measure its impact as well as assess compliance with relevant legal provisions, the organization's own internal regulations and the way standards on waste are devised and applied.

The bottom line for the audit will be a detailed consideration of the way the organization seeks to balance various competing social and business objectives. Company directors owe a duty to their shareholders to provide the best possible profit profile. This duty is also for the benefit of society as competing market forces equalize the production and distribution of goods and services. Businesses owe a wider duty to ensure that they operate in a fair and proper manner and in line with law. The mechanisms that enable this balancing act to result must be subject to audit coverage as a contribution to the future welfare of the organization. It becomes more serious where the organization is flouting laws and best practice, misleading the public and, at the extreme, falsifying test results on, say, levels of chemical waste. The new millennium is likely to see the growth of larger business concerns that emphasize a social conscience and where the audit role in promoting this policy receives much support.

Financial Systems Audit

Many think of internal audit as being primarily concerned with financial systems. This derives from the tradition of auditing, which prioritized financial matters as being key to accountability and thus

in need of ongoing verification and review. We have so far made little reference to the special role of financial systems since we view all operations as of importance to management and therefore the continuing welfare of the organization. This view is wholly defensible notwithstanding the fact that financial management may well feature in audit plans because of the high risk attached to this aspect of business activities. It would be wrong to leave our discussions of operational review without mention of the special nature of financially based systems:

Accountability Any managerial system of control must incorporate the key concept of managerial accountability. Here systems must be in place that record the results of business activities and account for what has occurred over a defined time period. Financial accountability is equally important since this sits well with entrusting budgeted resources with management, who must then account for the way this budget has been expended.

Front line work There are some financial systems that actually represent front line work and not just support services. Here, basic processing systems that account for income, debt, payments, grants and so on revolve around the finance arena. These constitute huge systems in their own right that may account for many millions of pounds of transactions that are processed in any one year. As such, they assume an importance for the audit plan and attract resources dedicated to ensuring that controls are in place and work. We accept that the external auditor does have a role in this matter although these systems are used as a short cut to verifying the figures in the final accounts.

Financial regulations Financial regulations and the financial management handbook are devices to ensure there are corporate standards over the way finances are administered across the organization. One model of internal audit suggests that it exists to promote adherence with the financial regulations issued by the director of finance. Internal audit follow these regulations within the organization and check that they are being applied as intended. This is relevant to remote locations that are a feature of geographically spread organizations that have branches in strategically located areas. The internal audit service has a distinctly financial flavour and this will feature in the plans, work and resulting reports. In one organization the finance manual has the following main sections:

Introduction	Background information
Staff responsibilities	Account code structure
Purchasing	Payments
Income	Receipts and subsistence
Petty cash	Wages and salaries
Finance computer system	Insurance procedures
Company credit cards	Useful accounting terms

Interrogations Financial systems are susceptible to wholesale interrogation where the relevant database may be tested extensively by the auditor. When tackling these types of systems, the application of suitable interrogation techniques is almost mandatory as a way of getting into the system and associated records. Any problems that are found not only indicate error but may also mean that the accounts are wrong or that fraud has been perpetrated, and these considerations have to be kept in mind by the auditor. Certain skills and techniques come into play as the auditor tackles large financial systems and these skills come at a premium. Not all auditors possess the right skills to take on these types of projects and an accounting background is definitely of use.

IS audit The IS auditor may assist the financial systems auditor in seeking to review and test large financial systems. Many of the IS auditor's skills are also relevant to the financial systems auditor as this type of work will also tend to involve automated systems.

Many operational auditors face the exciting prospect of reviewing complicated high-level operations that require a great deal of skill and care. This is the direction of internal audit as new and more important areas are tackled in the search for better performance and quality systems. Having said this, it is important that this search for new approaches does not mean we 'throw the baby out with the bathwater'. To this end, we cannot forget the importance of auditing the complicated financial systems that exist in all large organizations. Unfortunately, the operational auditors cannot generally perceive the value (and difficulty) of reviewing financial systems until they actually perform such an audit. The well-rounded auditor on the other hand has had exposure to financial and front-line operational systems during his/her career and this should certainly be encouraged.

Contract Audit

We have dedicated an entire section to IS audit on the basis that all large organizations will administer automated systems and techniques to support their business activities. Likewise, we might have discussed contract auditing using the same argument; that all organizations enter into contracts of some sort. In fact, we have not applied this approach since an open-ended review of the vast array of specialist audit areas would be never-ending. Internal auditors will be involved in an assortment of business systems depending on the nature of their organization and their approach to audit work. Financial services, housing associations, manufacturing companies, government departments, the service industry, pharmaceuticals, the health service and so on, each require some specialism in the type of operational field that features in the organization in question. These skills will be acquired over time as the auditor secures more and more relevant expertise. Hopefully, the application of audit techniques set with the theoretical framework of internal auditing will assist this task and provide a natural starting place for the field auditor. Contract audit is mentioned because there are several fundamental issues that can be of use in any audit role. These include:

Capital contracts The heyday of contract auditing developed after the Second World War when new build and major capital investment meant that structures and developments were a regular feature of business life. Reconstruction works led to extensive expenditure that had to be audited. The special skills required resulted in the employment of quantity surveyors, architects, designers, engineers and technicians in the internal audit department. Large contract audit sections appeared to support this. Nowadays, most organizations have moved away from an expansionist strategy, while new developments are not as frequent. The trend towards refurbishment means that major works will be based around refitting existing structures instead of new build. There are exceptions to this trend and one may still see building sites in many areas, particularly in cheaper, out-of-town locations. The contract auditor's work has had to change in recognition of these factors and it is within this context that we can list some of the relevant issues regarding this type of work.

Revenue contracts All large organizations enter into various revenue contracts as part of daily activities. These range from small contracts for the supply of stationery through to major ones for

computing services that are a key part of support services. The aggregate spend on contracts may be material and should appear in audit plans. A dynamic organization will resource a legal service that ensures these contracts are contained within a framework acceptable by the organization and not necessarily in the format of the supplier. Contract compliance and standards that cater for contract management are other features of a corporate approach that the auditor will seek to promote.

Link to purchasing The contract auditor will review the corporate purchasing policies and functions. Where local purchasing is the adopted model, there needs to be a firm framework of standards within which these spend decisions will be contained. This is over and above the more limited budgetary control procedures that should also be applied. European directives and international conventions bring with them a compliance flavour to the auditor's work, where operational management is at times simply unaware of the exact regulations that they must make reference to when preparing a new contract. This is also an area ripe for fraud and corruption where there are inadequate systems of control.

Externalized services Many new directors come into a post with a basic 'contract it out' viewpoint. This is seen as the answer to industrial unrest, poor performance, budget overspends and other adverse conditions. What many such individuals fail to appreciate is that this strategy, like all others, must be accompanied by suitable controls for it to work to any extent. If this approach is adopted, a complicated maze of contracts will be developed that interface across and throughout the organization, affecting many support and front line services. Without a major investment in contract management resources, which take on board service PIs, legal positions, accounting matters and contractual arrangements, and without ensuring the continuity of service delivery, these arrangements may simply fail. History records the number of service contracts that have ended up in arbitration or court action and this not only costs money but also involves disruption to services. It is not enough to build penalties into each contract since this is a last resort to punish the contractor. Effort directed at building good working relations with contractors based on clear terms of reference, close monitoring and ensuring both sides gain is a better solution. These and other associated matters should feature in the auditor's work and report.

Assimilated skills We need to mention the auditor's skills base and the way it is affected by contract arrangements that the organization has undertaken. The computer auditor, the financial systems auditor, the fraud investigator and probity auditor will each come across various major contracts during audit work. It is no longer possible to leave contracts as the province of the specialist contract auditor. The contracts skills base must be assimilated into the general field auditor's armoury of skills, knowledge and disciplines and this will be a growing feature.

Management is responsible for carrying out problem-solving enquiries and investigations into VFM, while audit can assist them. In contrast, audit are responsible for carrying out reviews of systems of risk management and internal control, and consultancy versus audit work should be seen within this context. There is much that all organizations need to consider when making sure that it is in compliance with legislation.

7.9 The Consulting Approach

Internal auditors have toyed with providing a form of internal consulting service for many years. The IIA standards now make it crystal clear that internal audit may provide consultancy as well

as assurance work to an organization. The IIA's handbook *Implementing the Professional Practices Framework* suggests six types of consulting work:

1. **Formal engagements –** planned and written agreement;
2. **Informal engagement –** routine information exchange and participation in projects, meetings and so on;
3. **Emergency services –** temporary help and special requests;
4. **Assessment services –** information to management to help them make decisions, for example, proposed new system or contractor;
5. **Facilitation services –** for improvement, for example, CSA, benchmarking, planning support;
6. **Remedial services –** to assume a direct role to prevent or remediate a problem, for example, training in risk management, internal control, compliance issues drafting policies.[54]

It is important to make clear exactly what constitutes consulting work since IIA Attribute Standard 1000.C1 says 'The nature of consulting services should be defined in the charter.' One difficulty is type one consulting which consists of a formal engagement with a planned and written agreement. The IIA handbook series goes on to distinguish between optional consulting work and mandatory assurance services:

> Assurance – adequacy of entity internal control, adequacy of process or sub-entity internal control, adequacy of ERM, adequacy of governance process, compliance with laws or regulations.
>
> Consulting – improvement in efficiency or effectiveness, assistance in design of corrective actions, controls needed for new systems design, benchmarking.

We need to turn to the management consulting professionals to gain an insight into the type of approach that may be considered for formal consulting projects. One well-known approach to consulting assignments involves the following basic sequences:

1. **Entry –** background work, initial contact with the client, preliminary survey (what is the problem?);
2. **Terms of reference –** width and depth, timescales, resources and reporting lines: make clear the requirements of Performance Standard 2120.C1, which states that 'during consulting engagements, internal auditors must address risk consistent with the engagement's objectives and should be alert to the existence of other significant risks'; also make clear corresponding roles and whether the work involves helping people do the analysis and solve their business problems, or whether it is more about tackling the problem and making recommendations to the client on ways forward;
3. **Contract –** in writing, why assignment needed, terms of reference (TOR), what will be examined, action to be taken to interested persons, agree on respective roles, support and implementing recommendations – who does what; monitoring arrangements for the project and reporting lines and planning and monitoring; it may also be an idea to build in any confidentiality clause and the contents of IIA Performance Standard 2130.C2, which states that 'Internal auditors must incorporate knowledge of controls gained from consulting engagements into the process of identifying and evaluating significant risk exposures of the organization.'
4. **Analysis –** covering:
   - **Diagnosis –** weigh up the evidence, what is acceptable, alternative solutions, computerization, what is most cost effective, policy constraints and then decision-making;

- **Planning for action –** firm recommendations, based on findings, policy and social considerations, reaction of client, rate of IT development, impact on VFM, participative approach, preliminary report, verbal report;
- **Implementation –** management responsible for implementation, routine follow-up after six months: how much we should support management in implementation – implementation must be planned watching for staff reactions; consultant may be available to help train staff (train small group who then train bigger groups), help anticipate problems, help develop action plan and checkpoints, but should not usurp management – need to set date when consultant's involvement stops; Also to make sure senior management is involved in more complex projects.

5. **Release –** from the contract when all work has been completed.

The value-added proposition is that the internal auditor can add a freshness of view and comes without the inbuilt assumptions of the people who operate the business line. These new insights have been described by Milan Kubr:

> It could be objected that managers, too, need to possess this range of knowledge and skills, and that each management situation is unique. What then can be gained by bringing in a newcomer who is not familiar with a given situation?
>
> Over the years, management consultants pass through many organizations and learn how to use experience from previous assignments in helping their new clients, or their old clients, to face new situations. Because they are exposed to many varying combinations of circumstances, consultants learn how to discern general trends and common causes of problems, with a good chance of finding an appropriate solution; they also learn how to approach new problems and opportunities. In addition, professional consultants continuously keep abreast of management literature and of developments in management concepts, methods and systems, including those taking place in universities and research institutions. Thus they function as a link between the theory and practice of management[55]

A further model of consulting investigations has been developed by the author and consists of a procedure involving 10 basic steps as shown in Figure 7.34.

[1] Initial terms of reference for the work

[2] Preliminary survey

[3] Establish suppositions

[4] Audit planning and work programme

[5] Detailed field work

[6] Determine underlying causes of problems

[7] Define and evaluate available options

[8] Test selected options

[9] Discuss with management

[10] Report

FIGURE 7.34 Performing consulting investigations.

[1] Initial terms of reference for the work

- Conduct key manager briefing and discussions on the review
- Outline symptoms and main problem areas
- Establish management success criteria
- Document brief history on events relevant to the issue in hand
- Indicate specific constraints acknowledged by management
- Look into management policy on unacceptable solutions, for example, staff cuts or major restructuring
- Indicate future plans that management has set for short and medium terms.

We establish a framework for the exercise, scope of the review and an indication of management need.

[2] Preliminary survey

- Committee/board minutes that impact on the review
- Brief discussions with staff to assess general consistency with key problems
- PIs
- Analysis of symptoms to capture 'what is really wrong'
- Internal reports and budgets
- Relevant published research that relates to the particular field of work
- Visit to the location.

We define the problems in detail and establish outline suppositions based on these problems (i.e. a range of possible causes).

[3] Establish suppositions

- Effects of the problems on performance, quality and VFM
- Materiality of the problems
- Hierarchy of suppositions: the most significant ones first
- Indications of how the suppositions may be tested to establish whether they are correct or not
- Likely causes of problems (based around the suppositions)
- Overall extent of the problems.

We must agree with management on what the problems are, their likely causes and how they will be tackled in the review.

[4] Audit planning and work programme

- Number of auditors required and time budgets
- Levels and types of expertise required
- Supervision of staff assigned to the project; how often and how this will be done
- Guidance on testing
- Review arrangements covering audit work as it is performed
- Reporting arrangements

- Programme of work (much will consist of research and testing)
- Time available and deadlines: for longer projects it is good practice to set milestones with defined products and progress review points
- Administrative arrangements including travel, expenses, accommodation, computers, and so on.

It is possible to set a clear progress checklist of underlying tasks and dates that can be monitored over the duration of the project.

[5] Detailed field work

- Programmed interviews
- Available research that will have to be secured and taken on board
- Re-performance of specific tasks if required
- Independent expert opinion where appropriate
- Inspection
- Cause-and-effect analysis
- Statistical analysis
- Questionnaires
- Construction of new PIs if required
- Other specific testing routines.

The aim is to establish whether the original suppositions are correct. This means securing sufficient reliable evidence.

[6] Determine underlying causes of problems

- Detailed discussions with management
- Review of managerial structures
- Review of existing managerial practices
- Determination of the extent of influence of the external environment
- Level of managerial control and guidance available to staff
- Establishing a clear relationship between problems and causes
- Distinguishing between symptoms and these underlying causes.

We will find out why these problems arose in the first place without necessarily assigning blame.

[7] Define and evaluate available options

- Extensive research in isolating suitable options
- Ideas from managers and staff
- Textbook solutions to form a starting place
- Model building
- The application of creative thinking
- Determination of relevant best practice elsewhere that is transferable.

The more options available the better, so long as they are feasible.

[8] Test selected options

- Defined benefits
- Staff expertise available and required
- Actual financial costs
- General resource implications
- Motivational aspects and impact on work flows
- Timetable for implementation
- Political aspects
- Knock-on effects for other systems
- Incremental improvements or the more risky 'big bang' approach
- Overall impact on 'the problem'
- Whether it complies with the fundamental 'rules' of successful change management.

We must remember that there is no 100% solution.

[9] Discussion with management

- Constraints that confront management, including practicalities
- Agreement on the factual content of report
- Bear in mind the costs of the audit and the need to provide a defined benefit
- Watch the psychology of negotiations – for example, seek partial compromise where necessary
- Keep in mind managerial objectives and their real success criteria
- Consider level of work carried out and the extent to which we can be sure of our position
- Consider overall acceptability of the audit work.

It is best practice to provide an oral presentation to top management where there are major implications from the review and the associated recommendations.

[10] Report

- The report should be formally cleared for final publication
- It should ideally be an extension of the oral presentation
- It should be ensured that the report is factually correct
- All managerial input should be properly reflected
- Report structure should be good and well written.

The required management action should be wholly clear and we would hope to have passed responsibility over to management and sold our ideas to them by the time the report is issued. A standard report structure may appear as in Figure 7.35.

Managing Change

Change management is a discipline in itself alongside a growing recognition of the crucial role of clearly defined change strategies. Audit consultants are likewise primarily involved in the change process, through their concern for seeking improvements in risk management and control. Much of the consulting role for larger strategic projects will revolve around the change management role which is why a study of the basic principles of change management will certainly pay dividends

Introduction
The party commissioning the work
the fact that it is consultancy, the difference between VFM and systems

Background to the operation
This will normally include:
the main activities, brief history, previous reviews, main suppositions

Main findings
For each of the suppositions

Recommendations
Options should be defined stating, where appropriate, any quantified savings and the effect on official budgets

Appendices
May consist of performance indicators

FIGURE 7.35 Standard report structure.

for the internal auditor. It is clear that managers are beginning to adopt the view that poor performance can be rectified through positive and planned change. The public sector is one area that is going through a major and ongoing reform exercise in an attempt to promote efficiency, effectiveness and quality in the delivery of public services. By studying change as a topic, the auditor may be able to promote the use of change techniques by management within a specially devised strategy that allows them to manage and control the change process. In fact there is one view that suggests that the auditor may become the change agent who underpins the fundamental process of change. Within this context, audit consultancies may be a key part of management's attempts to engineer change, a point that must be fully recognized if these recommendations are to have any great impact.

The Need for Change

There is an established trend to the adaptive organic organization, which has the ability to change as competing factors alter and affect it. Key features that promote ongoing change include:

- growing impact of corporate governance and risk management;
- the availability of specialist experts who can advise on specific changes;
- knowledge and general skills located throughout the organization;
- more advisory communication as opposed to direct instructions;
- more commitment from employees;
- individual tasks resourced as and when required.

There are other practical reasons why organizations need to change:

1. Increasing competition means the flexible, ever-changing organization is now the norm.
2. More participation by employees and therefore increased innovation forms a firm foundation upon which change initiatives may be developed.
3. Pressures on financial resources provide the impetus for slimming down and restructuring periodically.
4. Problems interfacing different departments may generate a change formula.

5. Greater levels of professionalism provide access to expertise on change management. This may be seen as the 'MBA phenomenon' whereby newly qualified staff join organizations with a view to doing things in new and improved ways.
6. Better performance review mechanisms allow management to monitor performance and target resources in a way that is most conducive to the achievement of organizational objectives. This, however, is dependent on good underlying information systems.
7. The tendency to differentiate activities paves the way for process re-engineering to be applied. The business unit concept encourages a client-based approach to work where local managers can make most business decisions without reference to corporate approval mechanisms.
8. Better forecasting techniques again assist the forward-planning process, which in turn promotes management action that matches the activities with probable changes in the environment.
9. Technological changes and improved decision support information systems are also relevant to this overall trend.

The drive is towards greater efficiency and performance and the much-sought-after 'competitive edge'. It may be argued that the manager must now be an expert in change management regardless of the field he/she operates within. Furthermore, the internal auditor should, as a minimum, understand and support this expertise if he/she is not already a change consultant.

The Implications of Change and the HRM Programme

Change will tend to affect three main areas of the organization:

- **The structure.** This is expected with a trend towards changing, flatter organizations with decentralized chains of command and better work flows, along with closer contact with clients and customers.
- **The technology.** This includes capital equipment and tasks combined. The link between organizational structure and underlying technology is featured in the socio-technological systems school of thought. New technology is quickly brought in if it is thought that there is a service delivery advantage that may be secured, without being seen as a major issue.
- **The people.** Selection, training and reward schemes are being given increasing attention in the search for the right people. Organizations in the past have tried to 'fit' systems into people, but are now increasingly buying in people who fit into the systems. People are now required to change to survive, as jobs are no longer guaranteed.

It is possible to extend this model to cover evaluating major options with a material affect on the organization. In the past, management has considered options via two criteria:

1. Economic feasibility.
2. Social acceptability.

Change management requires management to consider a third dimension:

3. **The human relations implications.** Here each individual (and group of individuals) may be affected in terms of economical, social, personal and political implications. The workers now have an additional role over and above the operational functions, as they must now become a positive, interactive component of the change programme.

Management may react to signs of change by piecemeal modification. Alternatively, it may develop and resource a programme of change in line with a clear human resource management programme over and above mere training. A change agent should be appointed to facilitate this.

The Individual Cost–Benefit Analysis

Some writers argue that when a major change exercise is undertaken, each member of the organization tends to carry out individual cost–benefit analyses to identify gains and losses as illustrated in Table 7.2.

TABLE 7.2 Individual cost–benefit analysis.

Perceived gains	*Perceived losses*
More convenience	Personal inconvenience
Social gains in status	Social fears
Job satisfaction	Less job satisfaction
More security (more skills)	Insecurity
Economic gains	Economic losses
Better conditions	Longer hours

After weighing up each of these factors the individual will decide whether his/her support for the changes will be high or low. Remember that the level of support will vary depending on whether the person is part of top management, middle management or front-line staff. It is not unusual for a sense of loss to be experienced as a result of a planned change even where defined benefits will be received. In essence, this may be seen as a loss of the security that many people need, which is derived from a steady-state environment. The problem is that while security is sought after in times of turbulence, it is these same times that demand great change from an organization and herein lies the potential conflict. This factor may well dictate the degree to which the employee is involved in, or distanced from, the change decisions. Many senior managers make the mistake of assuming that changes will be temporary and not disruptive. As such they fail to install effective controls at an early stage in the process, in anticipation of these types of problems. Internal audit is ideally placed by being removed from the operational detail, to define the types of control requirements that arise from a programme, as well as pointing out barriers to effective performance.

Resistance to Change and Other Associated Problems

Where members of the organization have adopted a change resistance strategy there will be problems in implementing the changes. Justified resistance to change may derive from:

Uncertainty as to the effects of the changes through lack of information When new things emerge without any warning or information to put them into perspective, there is a natural tendency towards apprehension. The unknown holds fear for many people who do not thrive on uncertainty, but prefer to work in a controlled environment. This is why it is so important to keep management advised about audit findings before a formal draft report is put before it.

Unwillingness to give up existing benefits that are threatened by the planned changes We may seek to alter the balance of power through planned changes and there is a level of resistance that derives from protectionalism in terms of these powers. For example, the auditor may be concerned about the fact that only one IT support specialist has experience of a particular corporate application and an audit report may comment on this as constituting poor control. This is the correct position in terms of the welfare of the organization, but can lead to great resistance from the IT officer as it removes him or her from a position of great power.

Awareness of specific weaknesses/loopholes in the proposed changes There are times when operatives know far more about a particular work area than the people who are developing the change programmes. What appears at first sight to be resistance from front-line staff, may in practice be concerned about problems inherent in the changes themselves. For example, a new computer system that gives a very slow response time may create problems from operational staff that have not been fully appreciated by the project team responsible for implementing the new system.

There are many problems that can arise where there is a high level of resistance to planned changes that may threaten the entire change process if left unattended. The ensuing problems can result from a poorly planned change programme:

1. poor quality of work that impairs productivity, service delivery and performance;
2. strikes and other forms of overt industrial action;
3. persistent quarrelling among the workforce leading to a volatile atmosphere;
4. earnest hostility towards management akin to a 'work-to-rule' type of environment;
5. sabotage;
6. token support with no meaning or depth;
7. reduction in output affecting productivity levels;
8. computerphobia where new systems are rejected and manual methods held on to;
9. requests for transfers out of the affected areas and resignations;
10. anger from the workforce;
11. significant increase in the level of absences due to illness and stress;
12. increase in complaints from both staff and clients;
13. accident levels increasing;
14. insufficient leadership resulting in a lack of key decisions;
15. key tasks not properly defined, resulting in insufficient coordination;
16. poor MIS that do not show feedback on progress on planned changes;
17. inadequate training leading again to performance problems;
18. competing crises that divert resources to operational problems, which means that the change programme then takes a back seat as 'real-life' problems are addressed;
19. unforeseen problems that make the task much more difficult – the fact that it is very hard work may have been overlooked by all those involved;
20. delays in progress, leading to frustration and demotivation; where this continues, there is a tendency for top management to withdraw their support where the programme is not working, and disassociate themselves from a potential disaster.

Stemming from the individual cost–benefit analysis, many members of the organization may be convinced that the planned changes will not work. This can turn into confrontation with a

destructive win/lose stance. Confrontation with uncooperative staff is valid but is risky and may result in long-lasting lowering of morale. Management will have to decide whether the potential conflict can be managed through the existing machinery or whether new processes have to be devised. This should be kept under close review because, if the required mechanisms are not put into place, the programme may fail. There is nothing wrong with internal audit providing advice so long as it is conducive to the achievement of organizational objectives. We have stretched our definition of controls to cover arrangements to ensure objectives are achieved. We illustrate the need to manage change in Figure 7.36.

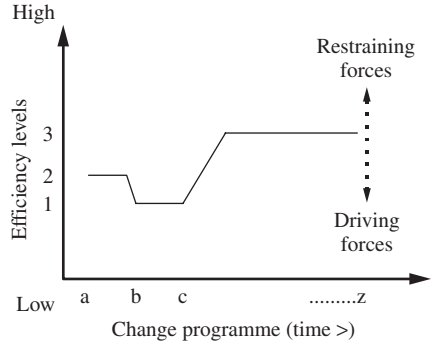


FIGURE 7.36 Efficiency levels and change.

The figure illustrates how the organization must be prepared to suffer a temporary drop in efficiency from level 2 to level 1 before level 3 is achieved. This problem will last from period b to c although the longer and deeper this curve, the longer the period and the more of a challenge the change programme will represent. In fact, the precise shape of the curve will be determined by the combination of both driving and restraining forces (see below). If change programmes are not carefully devised and managed they will be difficult to implement. Many organizations try to achieve too much over too short a time frame and this may cause an environment of unmanageable chaos.

A large organization brought in a new top management team. Their first initiatives were to implement a 25% staff downsizing programme and introduce performance appraisal for all staff. Most posts were deleted and the more capable officers applied for redundancy and left to pursue new careers. Staff with no qualifications had no option but to remain. Performance targets set just before the job cuts fell into disuse as turmoil and chaos resulted from the restructuring. The performance appraisal scheme was abandoned and the quality of services declined noticeably.

Force-field Analysis

There is much that occurs within an organization that is not set out in formal policies and procedures. Some have used as an illustration an organizational iceberg where formal overt goals,

structures, technologies, policies, procedures and resources are defined. However, this represents only the tip of the iceberg where a whole sea of informal covert perceptions, attitudes, feelings, values and group norms may be found below the surface. Any change strategy will have to recognize these hidden parts of the organizational iceberg for it to be effective. Kurt Lewin[56] has developed the force field as one way of analysing the competing pressures that drive and stop changes occurring. The idea is that the driving forces push for change so that the organization advances to a better position. The resisting forces, on the other hand, maintain an equilibrium by negating the power of these driving forces. Some of these driving forces are as follows:

- New IT and better systems create an almost unlimited scope to spot and develop change routines.
- Better materials can lead to faster and leaner production.
- Competition forces change and is perhaps the single most important driving factor.
- Supervisors' pressures for better performance are in line with a suitable strategic direction.

Resisting forces are as follows:

- Group norms for group performance can restrict the push for change.
- A genuine fear of change can add to this resistance.
- Complacency is a real dampener. The 'two years to retirement' syndrome is not conducive to any real change as a key manager seeks a containment position until he/she retires.
- Well-learned skills may become redundant and this may fall on the wrong side of the individual cost–benefit equation.

This model may be used to devise a master plan based on a strategy of enhancing the power of the driving forces while at the same time minimizing the impact of any resisting forces. A power audit may be used to isolate and so cater to the power bases that are affected by a change situation, particularly where an enhanced corporate computer system is being implemented. There is nothing wrong with the internal auditor performing such an exercise before embarking on the main change programme, as a way of weighing up the practicalities of a particular recommended course of action, before it is reported. The five stages of this power audit are as follows:

1. Analyse the existing political and cultural systems.
2. Assess likely changes in these power bases.
3. Consider the range of possible new operations and each one's effect on the power bases.
4. Assess the political and cultural problems in implementing each option.
5. Develop strategies for making a successful combination of options in terms of their political and cultural acceptability.

This may be seen as an ongoing process whereby particular problems are sensed and appropriate solutions then defined. The force field may be used to work on the driving and resisting forces. Where the power audit isolates attitudes that form resisting forces, a careful process of unfreezing the old and installing the required new attitudes must be actioned. The idea is that the old attitudes are unfrozen, changed, then refrozen as new attitudes. There are critics of the unfreeze/freeze/refreeze argument who see this as an artificial concept and this point must also be observed. Meanwhile, if we accept that old attitudes must be changed, we can set out a number of ways for unfreezing them:

- Show the effects of the existing problems to add an in-built acceptance of the need to change.

- Impress on staff the need for a competitive edge again as a forerunner to pending reforms.
- Gear the changes into a clear strategy that is known about and understood by staff.
- Provide suitable training programmes attaching to the required changes.
- Use staff counselling and ensure the required expertise is included within the change programme.
- Provide clear information on the proposed reforms.
- Define the necessity for all major changes to justify the need to secure improvement.

The Change Strategy

So far the change process has been built up using models and techniques that have been devised over the years. By spending resources on assessing the likely impact of proposed changes, we may define an appropriate change strategy. First and foremost, we may refer to the required changes and then ensure that the change strategy covers:

- how the structure may be changed with restructuring, decentralization and modified work flows;
- how the technology may be changed redesign work operations in line with good database and networking strategies;
- how both may be changed (i.e. techno-structural change) here structure and operations are redesigned together;
- how people may be changed in terms of their skills, attitudes and perceptions; alternatively, as a final option where all else fails, it may be necessary to change the actual people themselves.

The change strategy may move from a 'soft' through to a 'hard' approach depending on the degree of change, time available and the level of support secured. Where the anticipated level of resistance is high, one may wish to forgo the usual 'selling' techniques. Management may select a rigid, confrontational approach as a short cut to getting the changes implemented. Starting from the soft end, models have been developed to assess how confrontation moves through levels of severity as illustrated in Figure 7.37.

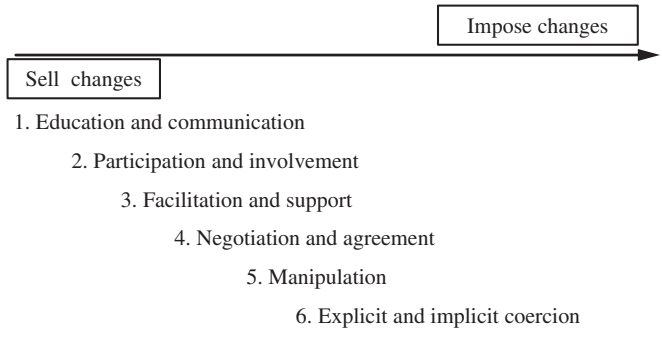


FIGURE 7.37 Degrees of confrontation.

Management must remember that the selected change strategy sets a precedent for future programmes.

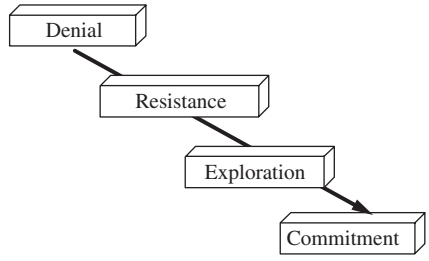


FIGURE 7.38 Moving from denial.

Dealing with Stress

Change and stress are intimately linked in that one may well lead to the other, particularly where the full impact of the changes has not been catered for. This then has a knock-on effect on the change programme and the ensuing performance of the staff involved. Colin Carnell has noted that:[57]

- new systems and processes have to be learnt and this takes time;
- new systems do not work perfectly at first but need modifying to improve performance;
- there is then an effect on self-esteem which may decline in times of change.

There is a view that performance will decline shortly after the changes are introduced as a result of the above-mentioned factors. The process of rebuilding the self-esteem then leads the drive for better performance and this task should be directed by senior management. Carnall goes on to describe a five-stage process where the changes are, in time, fully taken on board:

1. **Denial –** where the need for change is denied;
2. **Defence –** where one starts to face up to reality;
3. **Discarding –** where one now looks to the future;
4. **Adaptation –** where the challenges are met by building performance and overcoming setbacks;
5. **Internalization –** where new systems are created and new relationships accepted.

It is here that self-esteem can then be rebuilt as a foundation for improved performance by sound communications and understanding. The role of the manager is fundamental to the task of leading change and retaining the underlying sense of direction. Note that these ideas are taken from the work of Scott and Jaffe.[58]

Denial and resistance are the two main stages where stress may well develop and potentially lead to medical complications and it is here that support and reassurance is most required (see Figure 7.38 above). Certainly, we cannot turn to the issue of productivity until these early stages have been overcome and we have moved into the commitment arena. The principles, practices and techniques underlying organizational change should be studied and applied by management. The more resources applied to researching and using these techniques, the better placed the organization will be to meet competition. The auditor likewise must be prepared to become involved in this process as the audit presence can also contribute to the overall level of managerial stress, as an added pressure on both operational and senior management. Where the internal audit team does not possess the right competencies, which means it cannot perform consulting work to professional standards, such work should be declined.

Ensuring Technology Changes Are Well Managed

By Dan Swanson, Compliance Week Columnist

Information technology is critical to the long-term success of most organizations. It is a key reason for the cost of operations, and cost of operations tends to be a vital component of overall profitability. It facilitates the introduction of new business initiatives, as well as the ongoing improvement of current processes, and allows the management team to monitor and report on performance. IT enables business operations through connectivity, information processing, business intelligence, and the like. Lastly, and especially important to this audience, IT can contribute greatly to a company's system of internal control. With the organizational importance of IT continuing to grow each year, the importance of ''change management'' in IT systems continues to grow along with it. There is a substantial body of evidence that change management contributes critically to the implementation of efficient, effective, and secure IT operations. Because every change in an IT system creates a potential consequence on the company's operations, executives must understand change management thoroughly: how to impose it, how to enforce it, and how to monitor and improve its effectiveness. Research from the IT Process Institute has shown that organizations that manage their technology well perform substantially better than organizations that don't.

Simply stated, all IT changes need to be authorized and tested, and unauthorized or untested changes prohibited. Put another way: changes to a company's IT infrastructure are a significant source of risk for every business; to protect the corporate crown jewels, robust change management practices are absolutely critical. The need for a positive ''control environment'' within IT and an unforgiving attitude regarding unauthorized IT changes cannot be overstated.

Strong change management means planned system implementations, proven (read: tested) solutions, scheduled upgrade windows where recovery is facilitated if needed, and much more. To manage technology changes well, a change management program needs to be formally introduced into the organization. Implementing a change management program means assigning responsibility for the various change activities involved in implementing new technology solutions.

Auditing Technology Change Processes

An audit of change management should review IT results to identify key improvement opportunities. During the audit of change management programs, auditors need to:

- Understand the change management processes and procedures.
- Identify and assess key controls within the change management processes that ensure all changes are properly authorized and tested prior to implementation.
- Determine the quality of the information generated by the change management program, and assess whether it is sufficient to manage the change management process.
- Assess change management performance metrics for their existence, effectiveness, monitoring activities, and responses to any program deviations.
- Evaluate whether risk-management controls are preventive, detective, or corrective, and if a good balance has been implemented.

- Define tests to confirm the operational effectiveness of change management activities, including management and staff interviews, documentation and report reviews, and data analyses.
- Recommend opportunities for improvement of change management activities.

Indicators of Poor Change Management

- ***Unauthorized changes.*** Anything above zero is unacceptable. Establishing a tone at the top that clearly communicates the company's intolerance of unauthorized changes is fundamental to the long-term success of change management programs.
- ***Unplanned outages.*** System outages should be scheduled (planned) to reduce the impact on the organization's operations. Predetermined ''change windows'' are where production systems should be updated. Unplanned outages are caused by system problems and encourage a reactionary environment (that is, firefighting), which is not how you stay on top of internal control systems.
- ***Low change success rate.*** Good change management involves good testing; if changes have to be ''backed out,'' it is an indicator of poor testing that failed to catch problems in the early stages.
- ***High number of emergency changes.*** Again, emergencies should be emergencies, and happen infrequently. Poor planning of changes result in a high number of emergencies.
- ***Delayed project implementations.*** Delays in project implementation are a sign of unrealistic plans or poor resourcing decisions. Good change management practices encourage good planning and over time more achievable plans, resulting in fewer delays and cancellation of implementations.

An audit of change management should review the above risk indicators as a good measure of the likelihood that controls are or are not effective. Auditing IT processes can be very productive; good business results happen due to the quality of the processes used to produce them. Reviewing the policies and procedures and related processes that have been implemented will help determine if your IT investments will be productive and worthwhile. Also, discussing with IT management how they do their jobs – in particular their IT change efforts – will be extremely productive, and help answer the fundamental question: Are changes being implemented in a controlled or haphazard manner?

When I look at the work IT managers have done to test (that is, prove) that a change is working, I want to see four fundamental testing techniques: functional testing, stress testing, logical testing, and path testing. It has been my experience that if the above system testing isn't done, verified, and approved by some independent validation unit (quality control, internal audit, outside consultants, whatever), then we have a problem in 60 percent of the implementations.

Finally, a robust ''release management'' process, in addition to strong change management practices, should be the ultimate goal. Rigorous practices for building, testing, and issuing IT changes have a broad impact on individual IT results and overall performance of an organization. Therefore, while implementing a comprehensive change management program is important, establishing a strong release management process as well is strongly recommended.

IT Audit Guidance

The IT Compliance Institute has published a new IT audit checklist covering change management. This paper, ''IT Audit Checklist: Change Management,'' supports an internal audit of the organization's change management policies to verify compliance and look for opportunities to improve efficiency, effectiveness, and economy. The paper includes advice on assessing the existence and effectiveness of change management in project oversight, development, procurement, IT service testing, and IT operations; guidance for management and auditors on supporting change management; and information on ensuring continual improvement of change management efforts. Are your technology changes well managed? I believe it's time to find out.

Reprinted from *Compliance Week*. This article was originally published in Compliance Week. Reproduced by permission of Compliance Week. All rights reserved.

7.10 The 'Right' Structure

Once a clear audit strategy of risk-based assurance and consulting work is in place audit management must then turn its attention to the way resources are organized. This will have a crucial effect on the delivery of audit services. Furthermore, there are many options underpinning the type of structure that should be in place, which have to be considered and decided on. Some of these options are as follows:

- **Decentralized departments** may arise where the audit field consists of geographically isolated segments when it may be advisable to place an audit unit in each one. This can cover a region, country or even a whole continent, where the differences in local customs are so great that a centralized audit role would be inappropriate.
- **One centralized audit department** may be preferable where this is not the case. In contrast, the current trends to devolve financial management to line managers can also affect internal audit, who may be swept up in this strategy. Unfortunately, this will tend to dilute the power base of the CAE as stronger reporting lines are established with each department.
- **Service-based functions** may be divided into groups that provide specialized audit services such as IS, contracts, financial, consultancy, investigatory, regularity, risk-based systems and so on. The idea is to develop a level of expertise in particular audit services, in the search for enhanced professionalism. Another way is to split the assurance and consulting services. The setback is the degree of crossover that will arise where several auditors may emerge in the same work area, but with different objectives. It is also more difficult to establish a client-based view, as audit teams service the entire organization and not specified departments.
- **Client-based groups** are each responsible for a defined range of audit fields providing audit services for their main clients. Once an audit group has been assigned to a client (say, a director), we would expect a range of services to be provided as a contribution to developing the client/auditor relationship.
- **Mixed structures** arise where a combination of client- and service-based approaches is applied, and the audit field is allocated to groups that also provide some specialized services. This may reflect the practicalities of working life where clients are established for each audit manager, while there are some specialist audit services (such as fraud investigations) that will run across the organization.

- **A project-based approach** allows auditors to fall into a resource pool that forms into teams when audit projects demand. This is designed to provide a quick response-based service made up of floating expertise, and mirrors the multidisciplinary team approach where resources tackle problems as and when they arise. This can be an excellent solution but requires great skills to manage properly.
- **Consultancy-based models** are similar to the project-based one although auditors would work separately rather than in teams. This flat structure provides no client affiliation but can give a fast response time, particularly for unplanned work. An assignment is obtained, an audit brief and budget provided, and an auditor is sent out, to return with a draft report completed within budgeted hours.
- **Hierarchical structures** involve several tiers of auditors with a range of different grades each placed within defined audit groups. We may find an audit manager, principal auditors, senior auditors, audit assistants and then trainees. This traditional approach deems control to be inherent in all staff knowing their position in the audit unit and reporting lines clearly set and applied.
- **Project teaming** involves fixed audit groups but also selects individual auditors to form project teams for temporary assignments. Over and above this policy, auditors may be rotated between groups, say every three months, or have fixed-term secondments to specialized areas. Note that many groups that were originally set up as project teams become a permanent fixture.

Factors Influencing Structures

There are many choices and combinations of methods that may be applied and again, as with most of the material on audit management, a suitable decision must be made. This decision should be positive, based on the available options and founded on the overriding need to achieve a quality audit service. In practice, there is no one solution, although there are firm principles that should be applied along with a need to obtain a degree of inbuilt flexibility on the basis that change is now the norm. Furthermore, the audit structure should flow naturally from the agreed audit strategy. Once the CAE has set an agreed structure for the audit function and defined procedures and standards for the performance of audit work, then one might argue that staff should be able to deliver audit services as shown in Figure 7.39.

The quality of staff can be adjusted through the audit strategy but can depend on company policy.

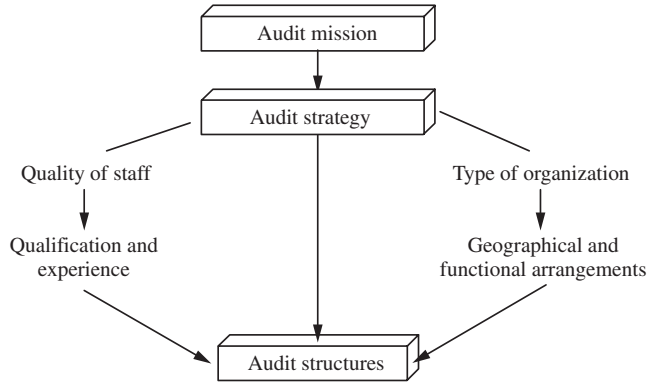


FIGURE 7.39 Structuring internal audit.

Status of Internal Audit

The status of internal audit has a knock-on effect on the level of independence that is secured. In an ideal world, one would argue that the higher the audit status, in terms of grades of staff, the better. This, however, does impose additional burdens on the CAE, not least being the high costs of running the services that will have to be recharged. Nonetheless, structuring must start with the actual position of internal audit in the organization and adopted reporting lines. There is also a link with status as shown in Figure 7.40.

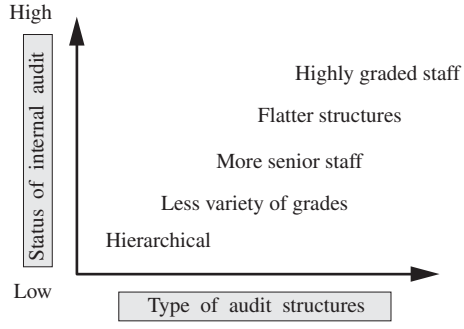


FIGURE 7.40 Audit status and structures.

Low-level audit work reporting to a fairly junior CAE (or audit manager) will result from low status and hierarchical structures will be the norm. High-level complicated audits of direct interest to the chief executive require the flatter, more response-based services provided by higher graded staff.

Individual Work

There is a conflict between the traditional auditor and the new style of working that has to be managed. The conventional working model is based on audit teams assigned to one project that could take many weeks. The team would consist of a senior auditor (or lead auditor) and one or more junior staff. The lead auditor would undertake systems evaluation and ascertainment while the juniors would tend to carry out the resultant testing programmes. A sense of team spirit would prevail and valuable experience in supervizing may be gained by the senior auditors. The juniors would meanwhile learn on the job and develop the necessary auditing skills as they moved up through the grades. In many audit departments, this model has given way to the new consultancy-based approach:

1. High-level audit work de-prioritizes the detailed testing that used to be carried out. Financial systems testing is done via interrogation software applied to downloaded databases.
2. Tight budgets are assigned to each audit to reflect the need for efficient use of resources. Clients pay directly for audit work and there is no excuse for assigning large teams to one audit.
3. One auditor would constitute the team and be required to complete the work within tight time frames. This person would have a great deal of control over the assignment, although the report would be cleared by audit management before publication.

4. This auditor works more or less alone and only uses juniors for specific testing when required. Additional staff arrive for, say, testing routines, and depart after the few days it would take to complete. The assigned auditor would be responsible for the results of this extra input.
5. In this way, the team concept is lost, but each audit is well delivered with the minimum costs and a focus retained by the assigned auditor.

One way in which some team spirit may be retained, alongside the application of the consultancy model, is for the audit manager to be a sounding board by discussing the project with the auditor. Another is to hold regular group meetings where each auditor may mention his/her project for limited debate. Finally, one might permit some exchange of views between staff as they discuss their specific audit (and any associated problems) when they are in the office. Unfortunately, the high cost of audit hours tends to mean that each auditor will have to perform his/her own audits from start to finish.

Project Teams

Project teaming is a useful way in which the audit department may build flexibility into its structure. This involves reassigning staff so that they group into a small team for a specific major project or series of projects. Alternatively, additional resources may be brought in to complement the existing staff, again for specific projects. This can be powerful particularly where additional consultancy services are being provided. Where management wants a particular exercise carried out, we may preserve our planned systems work and use project teams to resource an anti-fraud exercise or a major management investigation. If the project is so important, management will not mind funding these extra resources. A key auditor, say an audit manager, will have to direct the team's work so that it remains in control. Project teams can be resourced as follows:

Existing audit staff They will be reliable, but will not then be available to carry out planned audits. This approach may be perceived as treating audit as waiting around for real work to do, which does not promote a professional image. It will also be very difficult to plan work when staff are constantly being reassigned to project teams, unless the teams are part of the plans in the first place.

Employ consultants This is a very expensive option, although there will be less time spent reviewing their work. We would tend to use consultants for individual short-term projects and not for team-based work, which may last some time.

Employ agency staff This is a useful model as these additional resources may contribute directly to the project that would be managed by in-house auditors. Audit plans would remain intact and we can use the temporary staff for some time as they should not be charged at premium rates.

Second staff from elsewhere in the organization An excellent hand-picked team may be secured, although we must ensure that members' loyalties lie with the project. A training need may arise where this approach is applied and non-audit staff are used to any extent.

Employ people on short-term contracts The disadvantage is that confidentiality may become an issue where people who will not be staying with the organization are used on sensitive work. The main advantage is the flexibility that this creates where we may release staff as soon as their contract expires. We would be careful about investing excessive resources in training and development as this resource may be terminated in due course.

Allow the managers commissioning the project to supply the resources from their own establishment Here one may lose a degree of independence where, in the event of a conflict, loyalties may lie with the managers and not the organization. It is as well to set clear controls over the project team revolving around firm terms of reference, good review procedures and a tight budget for the work required. Remember that some staff may wish to engineer a permanent role for something that was only meant to be temporary.

Service-based Audit Teams

It is possible to set up audit teams or groups on the basis of the type of services that each group provides. This can be simplified in an example of four main audit groups specializing in:

1. Systems and IS audits
2. Risk management and CRSA
3. Consulting services
4. Investigations.

This is one way of developing expertise in specific audit areas. It is also possible to use the investigations team to avoid interrupting planned systems and probity work. One criticism of this approach is that client affiliation may be difficult to maintain where there is no one group responsible for one department. A contrasting approach is to set up groups for each of the main departments across the organization. This is illustrated in Figure 7.41.

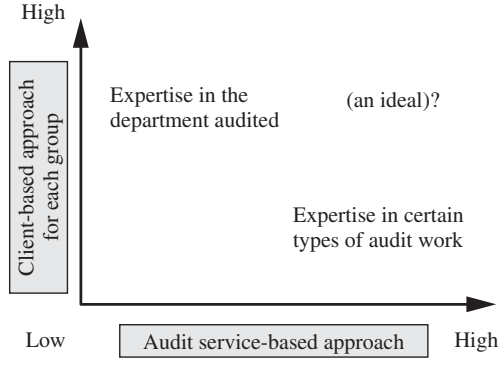


FIGURE 7.41 Client versus service-based teams.

We would have to consider the pros and cons of each approach and make a reasoned decision. It is possible to develop a mixed solution whereby audit groups are departmentally based but have an in-built specialism. This may appear as in Figure 7.42.

Audit groups may be assigned to departments while also being responsible for a defined type of audit service. This is made easier by relating the service to the department where this type of approach is most appropriate. The group would also be responsible for providing this service across departments. The investigations team would not be assigned to a department as problems of this nature could occur anywhere in the organization.

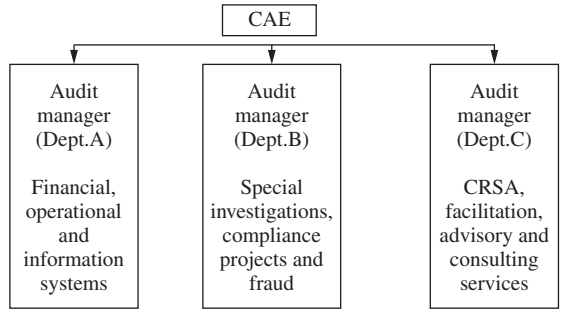


FIGURE 7.42 Departmentally-based teams.

Minimum Numbers

A discussion on how many staff need to be employed to support the audit mission will depend on the adopted audit strategy. This is not repeated here. What we have to address, however, is the fact that any audit structure will be determined by considering many factors; one of which is the number of auditors available to discharge the audit role. The larger the number of auditors the more temptation there is to develop a bureaucratic audit department with many tiers of staff and varying grades. As the number of staff increases over a certain limit, say five or six, one would have to consider developing the concept of audit groups. These groups would enable the CAE to divide the unit into manageable proportions headed by an audit manager (or group auditor). The freedom from staffing problems would then enable the CAE to deal with strategic matters that move the function from their existing position towards their targets/goals. In contrast, the CAE who has a section of fewer than five staff, will tend to assume a less strategic and more managerial role. The key point to note is that no fundamental answer to the question of how to structure the audit function can be provided. This is because the ideal position will depend on a variety of competing factors, including the audit strategy and the number of staff. If we are asked whether there is a minimum number of auditors that should be employed then one answer is:

> What is the minimum number of staff that should be employed to enable the CAE to hold senior management status and have a real impact on the organization?

An ideal position is reached where the audit function is seen as a major force in terms of its formal designation as a division or department rather than a small section or group. There is one caveat to this in terms of the need to ensure the audit budget does not become so large as to make this an excessively costly overhead to service managers. It may be an idea to take the views of the audit committee and the level of assurances that internal audit provide on internal controls. It is generally better to employ a small number of experienced auditors and focus on providing assurances for high-risk areas throughout the organization along with important consulting projects.

Supervisors

The audit structuring process cascades down from the CAE, audit managers through to senior auditors and other audit staff. The lead auditor/supervisor is a key officer in the audit world as it

is this person who, above all, produces the actual audit work. This fact should be fully recognized and catered to. Under the direction of an audit manager, the senior auditors should form the main unit that is assigned to the project either individually or as head of a small audit team.

Trainees

The bottom tier of the audit structure should ideally consist of trainees. These individuals will have limited experience in auditing matters but should be enthusiastic and form an inexpensive resource. It is good practice to use trainees as a source of future auditors and to ensure that we are up to date on new developments and research that comes with training programmes. Some audit departments do not necessarily employ 'trainees' but nonetheless encourage the less senior staff to undergo formal professional training. This is then built into their career development programmes.

We need to develop a sound model of the internal audit service with each auditor contributing to the work programme appropriately. Audit cannot be managed unless there are people working at the right level in the right capacity. The CAE has to keep a clear desk to formulate strategy and develop new and existing client bases. The audit manager should be able to run many projects at the same time while ensuring that each one meets quality standards that have been formally adopted. Auditors should be able to complete their audits in a competent manner to professional standards in line with the audit manual, and so generate the important fee income for the audit function. The structuring decision and underlying arrangements all contribute to the implementation of the most appropriate model that promotes the above position.

7.11 New Developments

In the past, the main characteristic of internal audit fieldwork was that the auditor was always very thorough. That meant, if the auditor did a stock check, he/she would count every item in his/her sample and track down anything that was missing or stored in the wrong place. The auditor would sit down and study detailed reports, carry out detailed analysis and would not stop until every question on the checklist was answered. The new risk management agenda means we accept some risk and we cannot give assurances on everything that happens within an organization. What is more relevant is that the auditor can give assurances on things that matter. Rather than being known as someone who can count every item of stock on the list, the auditor is becoming known as someone who is involved in governance issues that mean something to board members and strategic management. The other concern about fieldwork is that management is less interested in what happened in the past and more concerned about what is coming around the corner, and can the risk management process pick up these concerns and deal with them.

When considering the audit approach, it may be an idea to bear in mind the shortfalls that exist in many organizations. Many managers have no real grasp on the risks that they need to manage to stay on top. One survey brought home this worrying fact, and the key findings are reported below:

- Only half the internal auditors in our survey felt their organisations had a good understanding of the risks they faced, could prioritise those risks, and respond to them effectively.
- Some organisations have inadequate assurance over the risks they face and this will remain a problem because there is a significant shortage of people with internal audit skills.
- Internal auditors at the largest organisations are winning the argument for resources, but others must do more to make their case, especially if they want to expand their remit into areas where they believe their expertise is needed.[59]

There has been a long-running argument about the demands of auditing standards and whether smaller audit teams can meet the requirements of standards that appear to be aimed at larger units. There are some disadvantages where the audit team is fairly small but the more intimate atmosphere has some advantages as described by Nicola Rimmer:

> In a smaller team there is often less jockeying for position as can happen in larger teams, and so more of an opportunity for staff to get involved in audit planning and strategy, and make best practice suggestions and generally share knowledge. Also, if an individual has added value in a big way, this is more apparent, both within the team, but also amongst management, the audit committee and the board. This can provide invaluable experience for an internal auditor, although with the additional risk that they may quickly move on to bigger things. Whether working in a large or small audit team, each have their own particular challenges and advantages. However, large or small, the pressure on internal audit to deliver a quality service is increasing. One thing is clear – size really doesn't matter. What's important is how you use what you've got.[60]

One issue that has grown in importance over the years relates to the risk-based internal auditing approach that has seeped through into most internal audit units. Jeremy Opie has noted the benefits that come from using this approach:

1. Offers an independent and systematic basis for the organisation's stakeholders to judge the effectiveness of its internal control arrangements.
2. Provides the critical check that business objectives are clear and understood by all, and are congruent with the objectives of other parts of the organisation.
3. Provides an independent judgement on the effectiveness and efficiency of the risk identification and assessment process.
4. Provides an assurance of the accuracy, completeness and currency of the executive's risk picture.
5. Provides an assurance that the process for devising controls is effective and efficient, and equips the executive to manage change.
6. Provides an assurance that the executive's controls are effective and efficient, or an account of what is to be done to make them so; acknowledging, and giving due credit for, innovative management solutions to risk control. RBIA avoids merely imposing a standard control template.
7. Combats the risk of internal audit "doing management's job for them." Successful RBIA must work with management.
8. An RBIA programme should match the scope and objective of most annual internal control reports, offering valuable support to the reporting commitments of audit committees and executive boards.[61]

While risk-based auditing rules in most organizations, there is still a strong allegiance to building some compliance work inside many audits. Risk-based compliance reviews look at areas where the business may be breaking the rules, either through negligence, oversight, or through a degree of unchecked reckless behaviour that can place the entire business at risk. Risk-based audits examine the degree to which an operation is geared up to deal with risks to its future successful delivery, but that does not mean the auditor will want to ignore actual abuse that is happening right here and now.

Summary and Conclusions

The range and possibilities for internal auditor in terms of the services and approaches to their work are vast. This chapter has touched on some of these approaches and considered the specific issues and nuances of each approach. Internal audit work can be broken down into assurance-based and consulting-based work. A systems-based approach to assurance work can be related to reviewing higher-level systems such as the corporate governance system, the risk management system and the resulting systems of internal control. Moreover, assurance work can focus on various aspects of the control spectrum such as information systems, compliance issues, VFM and systems for protecting the corporate resource from fraud and abuse. Consulting work can also relate to each of the above areas, in that it can be geared to helping an organization set up its corporate governance arrangements including risk management and control. Consulting can also be used to drill down into these arrangements and involve facilitating risk events and workshops. Top-level consulting engagements may be programmed into the audit plans to tackle corporate and managerial problems and special investigations through a formal project that may take several months to complete. Ongoing efforts to provide advice and information to line managers may also be a feature of the internal audit role, again on a consulting basis. There has never been so much choice available for the internal auditor. The response to this dilemma is to talk to stakeholders, set a strategy, publish the results, ensure the right structure is designed and that audit staff are equipped to perform the strategy and then push ahead and monitor the success. It starts with setting the audit sights beyond what we used to do or what we have traditionally been good at. Real progress is made when the CAE is able to work 'outside the box' and develop a resource that really adds value to the direction, energies and accountabilities of the corporate body.

Chapter 7: Assignment Questions

Having worked through the chapter the following questions may be attempted (see Appendix A). Note that the question number relates to the section of the chapter that contains the relevant material.

1. Describe the concept of systems thinking and explain how this helps internal auditors adopt a defined approach to their work.
2. Explain how CRSA workshops may be designed and successfully delivered in an organization that is seeking to establish an effective risk management system.
3. Discuss the importance of facilitation skills in managing a CRSA workshop and describe some of the techniques for ensuring such workshops may be successfully facilitated to achieve their goals.
4. Consider the ways that audit may make use of the CRSA technique as an important component of audit field work and discuss why such an approach may prove beneficial.
5. Discuss the need for organizations to ensure the risk of fraud is properly managed and describe the various stages that may be considered when asked to investigate employee fraud.
6. Discuss the role of the IS auditor and note some of the controls that may help ensure an information system (e.g. an application such as a payments system) is both reliable, efficient and protected.

7. Explain why compliance is an important corporate issue and describe how an organization may ensure procedures are adhered to by managers and staff.
8. Explain the VFM concept and describe the link between economy, efficiency and effectiveness.
9. Describe how a formal consulting investigation (which involves a major change programme) may be approached and discuss how this differs from assurance-based audit work.
10. Prepare a presentation to the internal audit management team on the various ways that the internal audit shop may be organized and discuss whether there is one best method of structuring the audit service.

Chapter 7: Multi-choice Questions

7.1 Which statement is most appropriate?

a. Variety creates a richness and degree of flexibility in the type of audit work that is undertaken. In many cases, an audit department will contain different types of auditors who collectively discharge the audit function. Internal auditing is about evaluating management and this should be a central theme in most audit work.
b. Variety creates a richness and degree of flexibility in the type of audit work that is undertaken. In many cases, an audit department will contain different types of auditors who collectively discharge the audit function. Internal auditing is about evaluating risk management and internal controls and this should be a central theme in most audit work.
c. Variety creates a richness and degree of flexibility in the type of audit work that is undertaken. In many cases, an audit department will contain different types of auditors who individually discharge the audit function. Internal auditing is about evaluating risk management and external controls and this should be a central theme in most audit work.
d. Variety creates a richness and degree of flexibility in the type of audit work that is undertaken. In many cases, an audit department will contain different types of auditors who collectively discharge the audit function. Internal auditing is about evaluating risk management and internal controls, but this need not be a central theme in most audit work.

7.2 What is **x**?

There is an argument that the most efficient use of audit resources occurs where one concentrates on reviewing **x** as opposed to the examination of individual **x** transactions.

a. procedures
b. detail
c. systems
d. accounts

7.3 Insert the missing word/s:

The premise upon which the handbook is founded considers risk-based systems auditing as a valid interpretation of the assurance role of internal audit, with all other matters falling under the generic term, ... – most of which is part of the consulting service along with direct assistance and advice in establishing business risk management.

a. fact finding
b. evidential auditing
c. enquiries
d. investigations

7.4 Which is the most appropriate statement?

A system may be defined as:

a. a set of objects together with relationships between these objects and their attributes connected or related to each other in such a manner as to form an entirety or whole.
b. two sets of objects together with relationships between these objects and their attributes connected or related to each other in such a manner as to form an entirety or whole.
c. a set of objects together with relationships between these objects and their attributes connected or related to each other in such a manner as to form several units.
d. a set of objects together with relationships between these objects or their attributes connected or related to each other in such a manner as to form an entirety or whole.

7.5 Which statement is wrong?

There are a number of concepts that underpin systems theory and these various concepts may be listed:

a. connected components
b. unaffected by being in a system
c. assembly of components does something
d. assembly identified as being of special interest

7.6 Insert the missing words:

The ..... means that the whole process may be at risk where parts of the link are weak or break down. It is only by understanding the whole system that one is able to determine the effect of changes in any one area on other linked areas.

a. variable element
b. random fluctuations
c. series analysis
d. dependency chain

7.7 Which description a–e goes against which concept?

Systems concepts:	Description a, b, c, d or e
1. Managerial, operational and functional	
2. Parent system, main systems and subsystems	
3. Subjective system	
4. Systematic	
5. Systemic	

Descriptions of the above:

a. Here the use of a set system's boundary to define the system under review is something that auditors should apply to provide an agreed picture of what will be subject to audit.
b. The appreciation of systems relationships in a hierarchical manner, and as part of the associated system gives an insight into the way activities feed into each other.
c. The process of using a clear methodology is applied in systems-based auditing by using a defined methodology for planning, progressing the audit and then issuing the audit report.
d. The translation of systems to organizational levels and types gives a start to deciding how to break down the organization for audit purposes.
e. This use of systems theory is applied to the way the audit field is viewed as a series of systems and link systems.

7.8 What is this statement referring to?

This may be seen as a disorder, disorganization, lack of patterning or randomness of organization of systems.

a. randomness
b. entropy
c. inefficiency
d. collapse

7.9 Insert the missing words:
Systems are designed to process transactions and internal audit is concerned with controls that ensure the systems objectives are met. Where this does not happen, the system produces delinquent transactions that breach one or more of the five key control areas. An audit approach that ignores the systems but seeks to identify delinquent transactions may be seen as a ..... audit.
a. transactions-based
b. error-based
c. process-based
d. systems-based

7.10 Indicate whether the statements refer to a systems-based (SBA) or transactions-based approach (TBA)

a. Follow company vehicles to see whether they were being used on official business.	SBA or TBA
b. Observe several vehicles during the course of the audit to check the way these controls are operating.	SBA or TBA
c. Isolate and review controls over the process of preparing invoices and paying suppliers.	SBA or TBA
d. Examine a sample of payments to see if they are correct and proper without commenting on the underlying controls.	SBA or TBA

7.11 Insert the missing word:
..... controls are about the way people relate to each other and are motivated (or not). When systems are viewed as dynamic relationships, we can better understand the way control routines are developed and applied.
a. Complex
b. Dynamic
c. Flexible
d. Soft

7.12 Which three items are wrong?
It has been argued that systems-based auditing has a number of benefits:
a. It is positive and forward looking and considers the future strengths of control systems as opposed to isolating and reporting a series of past errors.
b. It promotes participation by involving the client in explaining the system and its objectives.
c. It promotes professionalism by churning out auditors who are experts in basic extensive testing routines.
d. It covers everything by being based on the system in operation.
e. It is constructive in seeking to improve systems.
f. It is preventive and views errors in terms of preventing them in the future rather than listing them for management to reprocess.
g. It can be geared into career development as an experienced systems auditor is able to tackle very complicated operations.
h. It promotes respect by requiring the auditor to understand the systems and the client's needs.
i. It develops auditors as experts in examining transactions rather than experts in reviewing risk management.
j. There is unlimited potential to extend systems auditing into all organizational activities.
k. Auditors generally find it more interesting with the emphasis away from testing transactions.

l. It can act as a vital aid to management with long-lasting effects in strengthening controls.
m. It can be a very efficient use of audit resources since it looks for causes of problems and not just the consequential errors.
n. Since it is error oriented, it is not therefore seen as negative by management.
o. It is systematic and key areas may be identified and isolated for further attention.
p. It has a wide scope and application and may be used to audit almost anything.

7.13 Which is the most appropriate statement?

a. Audit will ascertain the objectives and system to deliver these objectives, and evaluate whether the controls in place are able to handle the significant risks that get in the way of achieving the objectives. Testing will determine whether what should be happening is actually happening in practice and provide evidence to support the audit opinion.
b. Audit will ascertain the objectives and system to deliver these objectives, and evaluate whether the controls in place are able to handle the significant risks that get in the way of achieving the objectives. Evaluation will determine whether what should be happening is actually happening in practice and provide evidence to support the audit opinion.
c. Audit will redefine the objectives and system to deliver these objectives, and evaluate whether the controls in place are able to handle the significant risks that get in the way of achieving the objectives. Testing will determine whether what should be happening is actually happening in practice and provide evidence to support the audit opinion.
d. Audit will ascertain the objectives and system to deliver these objectives, and evaluate whether the controls that are planned are able to handle the significant risks that get in the way of achieving the objectives. Testing will determine whether what should be happening is actually happening in practice and provide evidence to support the audit opinion.

7.14 Which is the most appropriate statement?

a. Control risk self assessment is a tool that is used by businesses to promote risk management in teams, projects, through processes and generally throughout the organization. This tool is used by internal audit to help management.
b. Control risk self assessment is a tool that is used by businesses to promote audit routines in teams, projects, through processes and generally throughout the organization. This tool can be used by the executive board, partners, middle management, work teams and, of course, internal audit.
c. Control risk self assessment is a tool that is used by businesses to promote risk management in teams, projects, through processes and generally throughout the organization. This tool can be used by the executive board, partners, middle management, work teams and, of course, internal audit.
d. Control risk self assessment is a tool that is used by businesses to promote risk management in teams, projects, through processes and generally throughout private sector organizations. This tool can be used by the executive board, partners, middle management, work teams and, of course, internal audit.

7.15 Which description a–d goes against which type of workshop?

While in practice there are numerous types of CRSA events, we can suggest four basic approaches:

Types:	Description a, b, c or d
1. Process	
2. Projects	
3. People	
4. Preparedness	

Descriptions:

a. The emphasis is on protection of assets and containing any potential damage to the continued operation of the business.
b. The focus is on innovation and flexibility and the production of brand new controls that fit the bill.
c. The idea is to isolate the problems (risks) and solutions (controls) to encourage better performance.
d. The systems of internal control will tend to revolve around set procedures and information systems, that is 'hard controls to ensure things are done properly'.

7.16 Insert the missing word:

Many people have argued the value of CRSA:

What's so good about control and risk self assessment? It forces managers and their staff to think very carefully about their . . . . . and those of the organization.

a. values
b. objectives
c. motives
d. systems

7.17 Which statement is inappropriate?

People will participate and add to a CRSA workshop if they are . . . .:

a. committed to the workshop objective
b. have something of value to add
c. believe that their opinion will be appreciated
d. understand the CRSA process and where it fits into the business
e. are told the process is not part of continual improvement
f. have confidence in the way the workshop is applied

7.18 Which description a–d goes against which learning style?

Honey and Mumford have developed a learning cycle where people learn from their experiences and plan the next step from this learning. They have also classified different learning styles:

Style: Description a, b, c or d

1. Activist
2. Reflectors
3. Theorists
4. Pragmatists

Descriptions:

a. They like to see how things work in practice. They enjoy experimenting with new ideas. They are practical and down to earth, and like to solve problems; they appreciate the opportunity to try out what they have learned/are learning.
b. They see how things fit into an overall pattern. They are logical and objective 'systems' people who prefer a sequential approach to problems. They are analytical, pay great attention to detail and tend to be perfectionists.
c. They take direct action – are enthusiastic and like new challenges and experiences. They are less interested in the past or the broader context; they are mainly interested in the here and now. They like to have a go and try things out and participate – they like to be the centre of attraction.
d. They think things out in detail before taking action; they have a thoughtful approach, are good listeners and prefer to adopt a low profile. They are prepared to read and listen and welcome the opportunity to repeat a piece of learning.

7.19 Which statement is most appropriate?

a. Another way of viewing the workshop process is to suggest that the facilitator may assume a low profile early on as the idea of operational risk management and the CRSA process is sold to the group. As proceedings progress, the facilitator gradually moves into the foreground as the group become more confident about working without prompts.

b. Another way of viewing the workshop process is to suggest that the facilitator may assume a clear presence early on as the idea of operational risk management and the CRSA process is sold to the group. As proceedings progress, the facilitator gradually moves into the foreground as the group become more confident about working without prompts.

c. Another way of viewing the workshop process is to suggest that the facilitator may assume a clear presence early on as the idea of operational risk management and the CRSA process is sold to the group. As proceedings progress, the facilitator gradually moves into the background as the group become more confident and works so long as it is given prompts.

d. Another way of viewing the workshop process is to suggest that the facilitator may assume a clear presence early on as the idea of operational risk management and the CRSA process is sold to the group. As proceedings progress, the facilitator gradually moves into the background as the group become more confident of working without prompts.

7.20 Insert the missing word:

Some argue that this equation is important:

$$\text{Motive} + \text{Means} + \ldots = \text{Fraud}$$

a. desire
b. concealment
c. opportunity
d. collusion

7.21 Which item is wrong?

Frauds may:

a. be unintentional
b. be complicated
c. be simple
d. be one-off or continuous
e. be carefully planned
f. involve regular amounts
g. be perpetrated by senior officers
h. may involve large amounts

7.22 Which statement is least appropriate?

When employee fraud or irregularity comes to the attention of the auditor there are a number of alternative courses of action:

a. Call the police.
b. Search the employee's car.
c. Commence a management enquiry.
d. Commence an audit investigation.
e. Commence a joint management/internal audit investigation.
f. Interview the officer in question.
g. Suspend the suspect.
h. Instruct disciplinary proceedings.

i. Check the system of internal control.
j. Issue a formal instruction to staff.
k. Do nothing.

7.23 Which statement is most appropriate?

Surveillance involves observing the activities of defined individuals without their knowledge. Watching, looking and gathering evidence does not generally breach privacy standards and is a useful way of securing information in a fraud investigation:

a. It is sensitive and must be handled with care. One approach is to formulate a formal policy based on the premise that it should always be used at the start of an investigation. Some argue surveillance should only be carried out by experts. Simple undercover operations can yield results particularly where this is the only way of obtaining proof of a fraud.
b. It is sensitive and must be handled with care. One approach is to formulate a formal policy based on the premise that it should only be used when absolutely necessary. Some argue surveillance should only be carried out by experts. Simple undercover operations can yield results particularly where this is the only way of obtaining proof of a fraud.
c. It is sensitive and must be handled with care. One approach is to formulate a formal policy based on the premise that it should only be used when absolutely necessary. Some argue surveillance should only be carried out by auditors. Simple undercover operations can yield results particularly where this is the only way of obtaining proof of a fraud.
d. It is sensitive and must be handled with care. One approach is to formulate a formal policy based on the premise that it should only be used when absolutely necessary. Some argue surveillance should only be carried out by experts. Complex undercover operations can yield results and is a frequently used way of obtaining proof of a fraud.

7.24 Which statement is most appropriate?

The formal police caution in the UK runs as follows:

a. You do not have to say anything. But it may harm your defence if you do not mention something which you may later rely on in court. Anything you do say may be given in evidence.
b. You do not have to say anything. But anything you do say may be given in evidence.
c. You do not have to say anything. But it may harm your defence if you do not mention something which you may later remember. Anything you do say may be given in evidence.
d. You do not have to say anything. But it may harm your defence if you do not mention something which you may later rely on in court. Anything you do say will be written down and used by the prosecution.

7.25 Which statement is most appropriate?

Throughout the investigation interim reports should be issued setting out findings to date, implications and further work recommended:

a. It is for audit to suspend staff, instruct the police, search desks, confiscate books and records and the internal auditor should act in an advisory capacity. All major decisions should be made by audit under advice from experts.
b. It is for independent forensic experts to suspend staff, instruct the police, search desks, confiscate books and records and the internal auditor should act in an advisory capacity. All major decisions should be made by independent forensic experts under advice from internal audit.
c. It is for management to suspend staff, instruct the police, search desks, confiscate books and records and the internal auditor should act in an advisory capacity. All major decisions should be made by management under advice from internal audit.

d. It is for management to suspend staff, instruct the police, search desks, confiscate books and records and the internal auditor should act in an advisory capacity. All major decisions should be made by the Director of Finance under advice from internal audit.

7.26 Which statement is most appropriate?

All fraud reports should be clearly marked confidential. The number of copies should be restricted and it is best to present them on a need-to-know basis:

a. The report is not about giving an opinion of the guilt of the person, it is only to report the results of the investigation. The report may go on to state that there is sufficient evidence to support a case against a named suspect but it should not take a view on whether this person is guilty.
b. The report should give an opinion of the guilt of the person and report the results of the investigation. The report may go on to state that there is sufficient evidence to support a case against a named suspect and should take a view on whether this person is guilty.
c. The report is not about giving an opinion of the guilt of the person, it is only to report the impressions gained from the investigation. The report may go on to state that there is sufficient evidence to support a case against a named suspect but it should not take a fixed view on whether this person is guilty.
d. The report is not about giving an opinion of the guilt of the person, it is only to report the results of the investigation. The report may go on to state that there is sufficient evidence to support a case against a named suspect but it should only give the overall likelihood of whether this person is guilty.

7.27 Insert the missing words:

There tend to be two main results from fraud investigations. One is a referral to the police who will place a case before the Crown Prosecution Service with a view to bringing criminal proceedings against the parties in question. The other is that internal disciplinaries will be held against any employee where evidence points to their guilt in connection with the fraud. The first occurrence, requires a prosecution where the court will determine whether the defendant is guilty '.....', based on the evidence presented to it (and assuming the defendant pleads innocent). The second scenario requires the organization to bring charges of gross misconduct in front of a panel supported by evidence relating to these charges. The panel will judge on the less severe test of '.....' whether there has been a breach of internal discipline and then agree on a suitable remedy, which may result in dismissal.

a. "beyond reasonable doubt" and "balance of probability" (respectively)
b. "balance of probability" and "beyond reasonable doubt" (respectively)
c. "beyond some doubt" and "balance of probability" (respectively)
d. "beyond reasonable doubt" and "balance of 50% probability" (respectively)

7.28 Which two statements are least appropriate?

In terms of taking internal action against an employee, there are certain principles that should be followed:

a. Investigate and gather the facts carefully and compile the supporting evidence.
b. Be specific about the charges and let the employee know what the complaint is about.
c. Use counselling, training, support, for less serious problems that demonstrate a learning curve – employee fraud is unlikely to fall into this category as it will tend to be a gross misconduct.
d. Interview the employee and give him/her a chance to state his/her case. The employee should have a right to be accompanied by a trade union representative or colleague during any proceedings against him/her.

e. Introduce the evidence and explain where it came from and give the employee a chance to explain and clarify matters.
f. Determine the need to carry out further enquiries when given new information by the employee.
g. Convene an independent disciplinary hearing where both sides of the case are heard and witnesses examined and cross-examined before the panel adjourn to decide the case.
h. Make clear the decision to both sides.
i. Where the employee stays silent because there is an ongoing court case, then if evidence is sufficiently strong to require no explanation, the employer can go ahead with disciplinary action. The employee can only get an injunction to stop internal discipline where there would be a miscarriage of justice if it went ahead, which is quite rare. It is best to make the internal case about breach of procedure rather than use the terms 'fraud' or 'theft', which is what the criminal courts will be considering.
j. Make full records of the hearing and ensure that the only copy is filed confidentially on the employee's personnel record.
k. Provide an appeals mechanism where the employee is not satisfied that he/she has had a fair hearing.
l. An employee on remand has not committed an offence that has been proven so the internal case will have to be investigated. Where they have been given custodial sentence for an offence not related to their work, there may be grounds for dismissal especially if it makes the person unsuitable for the type of work performed or results in frustration of contract. Where an employee conceals a conviction that is not spent, he/she may be dismissed having forfeited the employer's trust.
m. The employer may give reference to a prospective new employer, but must not refer to the fact that the employee was facing unresolved disciplinary procedure.
n. The case may end up in an employment tribunal which is an independent judicial body comprising a legally qualified person as chairperson and two other members; one drawn from a panel of employer members while the other is drawn from a panel of employee members. In certain circumstances, a tribunal chairperson may sit without lay members.

7.29 List 10 attributes of good working papers (the handbook provides 24 examples).

Each fraud investigation must be recorded in a formal file that contains all the relevant documents that have been secured during the course of the investigation. There are a number of general attributes of good working papers that should be applied to these files:

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.

7.30 Which statement is least appropriate?

When acting as a witness, there are certain guidelines that should be observed by the auditor:

a. Make sure you are familiar with court procedure.
b. Refresh your memory by reading your statements.

c. Do not discuss your evidence.
d. Think before answering questions.
e. Try to help the prosecution prove their case.
f. Keep calm if the defence seeks to discredit your evidence.

7.31 Which two statements are least appropriate?

There must be an efficient implementation process whereby fraud response procedures are translated into action and results. A summary of the factors underpinning these procedures can be noted:

a. Let the procedures be based on a culture of fraud prevention.
b. Ensure that the organization has established an anti-fraud policy that is built into contracts of employment, management's role, director's priorities, and dealt with at induction training, ongoing training and development programmes.
c. The fraud investigation procedure may also be supported by formal fraud detection exercises where project teams are set up to isolate any particular frauds that are deemed to be of concern.
d. Train all employees in the investigations procedure.
e. Make sure the police are aware of our procedures and contact names and numbers.
f. Make the chief executive responsible for the fraud investigations procedure with advice from the chief internal auditor.
g. Adopt a formal policy of 'zero tolerance' where each time a problem arises we ask what went wrong, and who should be dismissed.
h. Ensure that there are effective mechanisms installed that mean that the investigations procedure is reviewed, kept up to date and properly applied across the organization.

7.32 Which three statements are least appropriate?

A disciplined approach is based on compiling sound evidence from reliable and confirmed sources with the resulting documents put together in a systematic fashion. Practical points to note:

a. The police prefer cases to be well presented with the evidence clearly compiled.
b. We should determine whether the enquiry is an internal disciplinary matter or a case for the police.
c. The police should be assigned a liaison officer which may be an internal auditor who will be in contact with them throughout the investigation.
d. When an allegation first comes to light, it is essential that the affected area is defined since any initial covert enquiries will have to be performed outside this area.
e. Where an employee is being investigated by the police as a result of an internal investigation, it is not possible to discipline this person.
f. When an employee is accused of stealing the organization's assets, it is important that the situation is quite clear.
g. The standard of evidence will be high since it will be scrutinized in detail at any later court hearing or internal disciplinary hearing.
h. It is best for audit to present disciplinaries and represent the organization in court while the management role may be reserved as that of principal witnesses.
i. Under the Data Protection Act 1984, non-disclosure does not apply where the information is needed to detect crime or apprehend or prosecute offenders.
j. The Advance Disclosure of Evidence Act stops defence from looking at witness statements before the case comes to trial.
k. When conducting an investigation, always open a file and adhere to the in-house standards.

7.33 Which statement is most appropriate?

a. There are differing views of IS audit with many believing that all audit sections should employ specialist auditors. Others feel there is no such animal as the IS auditor since tackling computerized applications is part of everyday audit life. Computer audit tends to be known as technical auditing, as we move from the idea of auditing computers to the view that we are helping to turn raw data into a reliable and secure platform for decision making.

b. There are differing views of IS audit with many believing that all audit sections should employ specialist auditors. Others feel there is no such animal as the IS auditor since tackling computerized applications is part of everyday audit life. Computer audit tends to be known as information systems auditing, as we move from the idea of auditing computers to the view that we are helping to turn raw data into a reliable and secure platform for decision making.

c. There are differing views of IS audit with many believing that all audit sections should employ specialist auditors. Others feel there is no such animal as the IS auditor since tackling computerized applications is part of everyday audit life. Computer audit tends to be known as information systems auditing, as we move from the idea of auditing computers to the view that we are helping to turn information into raw data as a reliable and secure platform for decision making.

d. There are differing views of IS audit with many believing that all audit sections should employ specialist auditors. Others feel there is no such animal as the IS auditor since tackling computerized applications requires specialist skills. Computer audit tends to be known as information systems auditing, as we move from the idea of auditing computers to the view that we are helping to turn raw data into a reliable and secure platform for decision making.

7.34 Which statement is least appropriate?

There are several options for securing the necessary IS/IT skills for internal auditing:

a. Use a consortium to provide the necessary skills.

b. Use a small number of IS auditors (perhaps one computer expert) to assist the other auditors as they tackle computerized systems.

c. Train general auditors in IS audit techniques.

d. Rotate auditors between groups with one group specializing in computerized systems.

e. Try to avoid considering the IS aspects when performing audit work.

f. Use consultants either to perform certain computer audit projects or to assist the general auditors.

g. View computer audit as the audit of MIS and apply a wider base to computer audit projects covering managerial controls as well as computerized ones.

7.35 Which statement is least appropriate?

In terms of managing IS audit resources note that:

a. A cycle of audits may be planned to cover all of the main computerized applications.

b. It will be necessary to set up a constructive liaison with the corporate IS managers.

c. The difficulties in recruiting good quality IS auditors have already been mentioned.

d. The depth of technical expertise should be defined in an appropriately worded job specification.

e. The timing of IS audit work has to be planned as systems tend to take turns in securing a high profile as the organization's strategy alters.

f. A budget for IS audit should include high-specification computer facilities along with notebooks, scanners, quality printers and so on, for use by auditors.

g. The audit manager cannot really carry out a proper review of the IS auditor's work, so this work may not always be properly supervised.
h. The work that IS audit performs on systems development may become part of the systems of internal control. As such, the role should be clearly defined at the outset.
i. IS auditors may spend time supporting the audit function by developing computer assisted audit techniques and the way this is resourced has to be agreed on via the audit plan.
j. Developing a comprehensive range of control matrices covering automated systems can aid control evaluation and this may well be an IS audit task.

7.36 Select the most appropriate description a–c for types of standby centres.

The organization should ensure that it has a contract for standby facilities to take over processing in the event of the computer centre becoming unusable. There may be three main types of contracts:

Type:	Description a, b or c
1. Cold standby centres	
2. Warm standby centres	
3. Hot standby centres	

Descriptions:

a. Here the facility would be readily available and be functional within a fairly short time.
b. One might either maintain an in-house facility into which servers might be moved or subscribe to an existing facility.
c. This facility, being the most expensive method, is set up with copies of the files dedicated to the system in question and may be operational at a moment's notice.

7.37 Which statement is least appropriate?

The IS auditor's role in disaster planning is to:

a. recommend that a plan is in place
b. independently test this plan
c. call out key contacts in the event of an emergency
d. review the contract with the facility's supplier along with any tendering arrangements
e. review the extent to which the plan is understood by all participants
f. advise the disaster committee on any security implications that may need to be addressed.

7.38 Indicate for each control whether it is best classified as an input control (IC), processing control (PC) or an output control (OC). Note that risks to computer applications are mitigated through input controls (on inputs to the system), processing controls (that are set within the underlying application software) and output controls (that relate to the outputs from the system).

1. access, security and passwords control
2. all expected output received
3. an adequate transaction trail available so that data may be traced to the original or and through the system
4. anti-virus software
5. appropriate format
6. authorization
7. batch control (where appropriate)
8. call back for remote access
9. check digits
10. checkpointing – saving transactions at a certain point in time
11. compatibility checks – consistent field used
12. completeness checks, for example, all fields covered and all data accounted for

13. completeness, for example, batch numbers
14. completeness schedules of expected output
15. control totals
16. control totals
17. controlled stationery
18. data being quickly resubmitted wherever necessary
19. disciplinary action with instant removals of staff
20. disposal of documents and reports
21. double keying and verification
22. duplicate input checks
23. encryption
24. error messages
25. error reports
26. e-transfers authorization
27. exception checks – for example, overtime only given to certain grades of officers
28. exception reports
29. exceptions investigated by a responsible officer
30. file identification controls
31. firewalls and authentication routines
32. format checks – that ensure the item is either alpha or numeric
33. good security arrangements for reports in line with data protection rules
34. independent check on all output
35. limit checks
36. logical routines
37. manual procedures to ensure all reports reach their destination
38. mechanisms to ensure that the output is received in a timely fashion
39. missing data checks
40. overflow flags that indicate where excess digits have been used
41. page numbering
42. physical access restrictions
43. prioritization of output
44. range checks – so that a transaction must be between say £0 and £20,000
45. reconciliation of related fields
46. record count
47. recovery procedure
48. reference documents
49. reports only sent to authorized users
50. rules on automated document retention and storage
51. run-to-run controls – for example, total gross pay from the Gross Pay programme should be the input to the Net Pay programme
52. screen viewing restricted to authorized personnel
53. secure printers
54. security over valuable stationery
55. segregation of duties
56. sequence checks on consecutive numbering
57. sequential numbers
58. shredders for confidential waste
59. staff training and recruitment

60. suitable reports
61. supervisors review and authorization
62. systems failure controls
63. the appropriate media used
64. the whole validation programme
65. turnaround documents
66. user feedback to ensure that reports are no longer sent where they are not used
67. user procedures
68. validation – range, format, reasonableness
69. validation (display data after routine) – accuracy checks
70. validity checks – say checking that a correct code has been used
71. well-designed input documents
72. well-planned error and exception reports
73. working documents.

7.39 Insert the missing word:

. . . . . is an issue for the internal auditor and during the audit, an assessment will be made of the extent to which the business is adhering to laws, regulations and control standards.

a. Compliance
b. Professionalism
c. Efficiency
d. Effectiveness

7.40 Which of the steps is inappropriate?

A procedure for carrying out probity audits is:

1. The work will be agreed with senior management and this may involve a one-off visit or a series of programmed visits.
2. The appropriate line manager should be contacted and a date set for the visit. It is possible to distribute an audit information brochure in advance of this visit.
3. It is possible to apply standardized documentation to this programmed audit work. Probity visits should not be allowed to consume excessive audit resources and the approach will be to apply junior staff wherever possible and work to tight budgets of up to, say a week. This will depend on the type of audit.
4. Visits to remote establishments/operations should include:
   a. a cash-up
   b. vouching a sample of transactions from the banking arrangements
   c. inventory checks covering all valuable and moveable items
   d. a check on a sample of local purchases and tests for compliance, integrity and effect on the cost centre
   e. a programme of tests applied to all areas that may be vulnerable to fraud or irregularity
   f. a check on the performance of operational staff to assess whether they are working efficiently, are being properly motivated and engender good team spirit
   g. verification of a sample of returns made to head office
   h. other checks as required or agreed with management.
5. The work undertaken will have to meet the standards set out in the audit manual and any appropriate documentation, and report format should be agreed with the audit manager.
6. The standards of review should comply with the audit manual, and supervisory review and performance appraisal documents should be used by audit management.

7.41 Select the most appropriate name a–c for the given descriptions 1–3.

Descriptions:

1. Resources required to perform the operation are acquired in the most cost-effective manner.
2. Resources are employed to maximize the resulting level of output.
3. Final output represents the product that the operation was set up to produce.

Names:

a. efficiency
b. effectiveness
c. economy

7.42 Select the most appropriate term (efficiency or economy) for items a–d.

A systems-based approach to an (a) review would consider the standards, plans, direction and type of information that management applies to controlling their operations. The investigative approach, on the other hand, concentrates on specific methods by which (b) may be improved. This may be by applying best practice in terms of alternative operational practices, or by isolating specific instances of waste and inefficiency that may be corrected. (c) (i.e. securing the cheapest inputs) is incorporated into the wider concept of (d) because of the intimate link between these two. Efficiency covers basic matters of economy.

a.
b.
c.
d.

7.43 Insert the missing word:

Much material may be gathered where the auditor compiles his/her own performance indicators (PIs) and thereby isolates potential poor performance. This may be carried out by:

- comparing similar operations,
- comparing one operation over defined time periods or
- considering variances between planned performance and the actual results.

This process may identify "……", that is, those areas where one may find a failure to secure good value for money.

a. evidence
b. findings
c. an opinion
d. suppositions

7.44 Insert the missing word:

The starting place for …… audit is to reassess the public image of the organization.

a. internal
b. social
c. efficiency
d. compliance

7.45 Which stage of the approach to performing consulting investigations is inappropriate?

a. Initial terms of reference for the work
b. Preliminary survey
c. Establish suppositions
d. Audit planning and work programme
e. Detailed field work
f. Determine underlying causes of problems
g. Define and evaluate available options
h. Implement selected options

i. Discuss with management
j. Report

7.46 Which practical reason that organizations need to change is inappropriate?

a. Increasing competition means the flexible, ever-changing organization is now the norm.
b. More participation by employees and therefore increased innovation forms a firm foundation upon which change initiatives may be developed.
c. Pressures on financial resources provide the impetus for less innovation and more entrenched structures.
d. Problems interfacing different departments may generate a change formula.
e. Greater levels of professionalism provide access to expertise on change management. This may be seen as the 'MBA phenomenon' whereby newly qualified staff join organizations with a view to doing things in new and improved ways.
f. Better performance review mechanisms allow management to monitor performance and target resources in a way that is most conducive to the achievement of organizational objectives. This, however, is dependent on good underlying information systems.
g. The tendency to differentiate activities paves the way for process re-engineering to be applied. The business unit concept encourages a client-based approach to work where local managers can make most business decisions without reference to corporate approval mechanisms.
h. Better forecasting techniques again assist the forward-planning process which, in turn, promotes management action that matches the activities with probable changes in the environment.
i. Technological changes and improved decision support information systems are also relevant to this overall trend.

7.47 Insert the missing word:

It is possible to extend this model to cover evaluating major options with a material affect on the organization. In the past, management has considered options via two-dimensional criteria:

1. **Economic feasibility**.
2. **Social acceptability**.

Change management requires management to consider a third dimension:

3. **The ..... implications.** Here each individual (and group of individuals) may be affected in terms of economical, social, personal and political implications. The workers now have an additional role over and above the operational functions, as they must now become a positive, interactive component of the change programme.

a. audit
b. human relations
c. structuring
d. performance

7.48 Which statement is inappropriate?

Where members of the organization have adopted a change resistance strategy there will be problems in implementing the changes. Justified resistance to change may derive from:

a. Uncertainty as to the effects of the changes through lack of information.
b. Unwillingness to give up existing benefits that are threatened by the planned changes.
c. Awareness of specific weaknesses/loopholes in the proposed changes.
d. Change would require a great deal of effort.

7.49 The driving forces push for change so that the organization advances to a better position. The resisting forces on the other hand, maintain an equilibrium by negating the power of these driving forces. Indicate for each force whether it is a driver (D) or a resister (R):
   a. A genuine fear of change can add to this resistance.
   b. Better materials can lead to faster and leaner production.
   c. Competition forces change and is perhaps the single most important driving factor.
   d. Complacency is a real dampener. The "two years to retirement' syndrome is not conducive to any real change as a key manager seeks a containment position until he/she retires.
   e. Group norms for group performance may restrict the push for change.
   f. New IT and better systems create an almost unlimited scope to spot and develop change routines.
   g. Supervisors' pressures for better performance that are in line with a suitable strategic direction.
   h. Well-learned skills that may become redundant and this may fall on the wrong side of the individual cost–benefit equation.

7.50 Which structure is inappropriate?
   Furthermore, there are many options underpinning the type of structure that should be in place, which have to be considered and decided on. Some of these options for structuring the internal audit department are:
   a. Decentralization
   b. Centralization
   c. Service-based
   d. Client-based
   e. Mixed structures
   f. Performance-based
   g. A project-based approach
   h. Consultancy-based
   i. Hierarchical structures
   j. Project teaming

References

1. O'Connor Joseph and McDermott Ian (1997) 'The art of systems thinking', Thorsons, p. 25.
2. *Evening Standard*, Tuesday 5 Nov. 2000, p. 16, 'Blunkett urged to act on student visa fraud', Hennessy Patrick.
3. O'Connor Joseph and McDermott Ian (1997) 'The art of systems thinking', Thorsons, p. 41.
4. O'Connor Joseph and McDermott Ian (1997) 'The art of systems thinking', Thorsons.
5. O'Connor Joseph and McDermott Ian (1997) 'The art of systems thinking', Thorsons, p. 7.
6. O'Connor Joseph and McDermott Ian (1997) 'The art of systems thinking', Thorsons, p. 17.
7. O'Connor Joseph and McDermott Ian (1997) 'The art of systems thinking', Thorsons, p. 13.
8. O'Connor Joseph and McDermott Ian (1997) 'The art of systems thinking', Thorsons, p. 143.
9. O'Connor Joseph and McDermott Ian (1997) 'The art of systems thinking', Thorsons, p. 85.
10. IIA, 'Internal auditing alert', May 1998, 'Validating CSA – a "how to" interview with James Roth'.
11. IIA, 'Professional practices pamphlet', 1998-2, 'A perspective on control self-assessment'.
12. 'Control self assessment overview, MC2 management consulting, control and risk self assessment', McNamee, David (www.Mc2consulting.com), accessed 2005.
13. IIA, 'Professional practices pamphlet', 1998-2, 'A perspective on control self-assessment', p. 221.

14. Oxley Tom, 'A new approach to control and risk management – Part II'. *Internal Auditing*, May 1993.
15. IIA, 'Professional practices pamphlet', 1998-2, 'A perspective on control self-assessment'.
16. Professional Briefing Note, Control and Risk Self Assessment Fourteen, 1999.
17. O'Connor Joseph and McDermott Ian (1997) 'The art of systems thinking', Thorsons, p. 85.
18. Pidzamecky Mike, 'CSA according to Mike, is CSA dead?', *CSA Sentinel*, October 2001, Vol. 5, No. 3.
19. Chambers Andrew (2002) *Corporate Governance Handbook*, Tolley's Reed Elsevier (UK) Ltd, p. 317.
20. Hart Lois B. (1992) 'Faultless facilitation', London, p. 19, Kogan Page.
21. Heron John (1998) *The Facilitators Handbook*, p. 15, Kogan Page.
22. Taraschi Rosaria, 'Cutting the ties that bind', *Training and Development*, Nov. 1998, pp. 12–14.
23. O'Connor Joseph and McDermott Ian (1997) 'The art of systems thinking', Thorsons, p. 65.
24. Lacoursiere R.B. (1980) *The Life Cycle of Groups: Group Developmental State Theory*, New York: Human Services Press.
25. Chambers Andrew (2002) *Corporate Governance Handbook*, Tolley's, Reed Elsevier (UK) Ltd, p. 313.
26. CIPFA (1994) *The investigation of fraud in the public sector*, 2nd edition, p. 1.
27. Weait Mathew, 'The workplace ethic is it a crime?', *Management Today*, Jan. 2001, pp. 53–57.
28. Carpenter Brian W. and Mahoney Daniel P., Ernst & Young Survey, 'Analysing organizational fraud'. *Internal Auditor*, May 2000 – The Unmanaged Risk: An International Survey of the Effect of Fraud on Business, pp. 33–38.
29. The White Paper, *Journal of The ACFE*, 2002 Report to the Nation – The Wells Report.
30. Whitehead Mark, 'Research into fraud points finger at middle managers'. *People Management*, 14 Jan. 1999.
31. Dittenhofer Mort, 'The behavioural aspects of fraud and embezzlement'. *Internal Auditing*, July 1990, pp. 13–19.
32. HM Treasury, Auditorium, Spring 2000–2001 Government Fraud Report, pp. 2–3.
33. 'Cybercrime survey 2001', Confederation of British Industry, *Internal Auditing and Business Risk*, 2001, p. 20.
34. Hunter Mark, 'Money Laundering'. *Internal Auditing*, May 2000, p. 19.
35. The White Paper, *Journal of The ACFE*, 2002 Report to the Nation – The Wells Report.
36. The White Paper, *Journal of The ACFE*, 2002 Report to the Nation – The Wells Report, 'CFES indicate fraud rate may be stable', p. 31.
37. HM Treasury Auditorium, Spring 2000–2001 Government Fraud Report, pp. 2–3.
38. Position Paper, ECIIA, 'The internal auditor's role in the prevention of fraud', Oct. 1999.
39. ECIIA European Confederation of Institutes of Internal Auditing, Press Release, Position Paper, 'Internal audit's role in the prevention of fraud', 1999.
40. Heinman-Hoffman, Morgan and Patton, 'The warning signs of fraudulent financial reporting'. *Journal of Accountancy*, Oct. 1996, Reported in the *CFE Fraud Examiners Manual* 1998.
41. 'Internal auditing and business risk', Nov. 2002, pp. 32–33.
42. *Internal Auditing*, March 1998, p. 10.
43. Sawyer Lawrence B. and Dittenhofer Mortimer A., assisted by Scheiner James H., 1996 *Sawyer's Internal Auditing*, 4th edition, Florida: The Institute of Internal Auditors, p. 1199.
44. Cowan Neil, 'Company-wide fraud offensive'. *Internal Auditor*, April 2000, In My Opinion, p. 88.
45. Moeller Robert and Witt Herbert (1999) *Brink's Modern Internal Auditing*, 5th edition, New York: John Wiley and Sons Inc, p. 612.
46. Kolman Mark R. 'Living dangerously'. *Internal Auditing*, June 2002, p. 72.
47. McCollum, T. 'Cyber-crime still on the rise'. *Internal Auditing* – Loose, June 2002, pp. 16–17.
48. IS Auditing Guideline, Use of Risk Assessment in Audit Planning, Standard Effective from 1 Sept. 2000.
49. IT Disaster Recovery, a Guide for Internal Auditors, Information Technology Briefing Note, 2001, p. 26, para. 12.2.
50. *Daily Mail*, 3 Sept. 1996.
51. *People Management*, 11 July 2002, pp. 46–47.
52. Shapiro Elaine C. (1996) *Fad Surfing in the Boardroom*, Capstone Publishing Ltd, p. 219.
53. *VFM Audit Manual*, Office of the Auditor General of Canada, Oct. 2001.
54. Anderson Urton and Chapman Christy (2002) 'The IIA handbook series' in *Implementing The Professional Practices Framework*, IIA, p. 21.

55. Milan Kubr (ed.) (1986) *Management Consulting, a Guide to the Profession*, 2nd edition, International Labour Organisation.
56. Lewin, K. (1951) 'Field theory in social science, selected theoretical papers', Harpers and Brothers.
57. Carnell, C. (1991) *Managing Change*, Routledge.
58. Scott C.D. and Jaffe D.T. (1989) 'Managing organisational change', Kogan Page.
59. Towards a blueprint for the internal audit profession, Research by the Institute of Internal Auditors, page 7 – UK and Ireland in association with Deloitte, Deloitte & Touche and the Institute of Internal Auditors – UK and Ireland 2008.
60. Internal Auditing & Business Risk, IIA Magazine, Size isn't everything, September 2007, page 35, Nicola Rimmer
61. IIA Journal, January 2008, Internal Auditing & Business Risk, 39, Jeremy Opie.

Chapter 8

SETTING AN AUDIT STRATEGY

Introduction

The previous chapters of the Handbook have reflected the major challenges that face internal auditors as they seek to add value to their employers. The 'value add' proposition is a main driver for the audit services and choices need to be made in terms of what is delivered by internal audit and how this task is achieved. The IIA's Performance Standards 2000 (Managing the Internal Audit Activity) reinforces this concept by stating that: 'The CAE must effectively manage the internal audit activity to ensure it adds value to the organisation.' The most important factor in this equation is the audit strategy that is set to achieve added value. Added value is described by the IIA in the following way:

> Value is provided by improving opportunities to achieve organizational objectives, identifying operational improvement, and/or reducing risk exposure through both assurance and consulting services.

The CAE will succeed or fail on the basis of the adopted audit strategy and the crucial role of strategy has been eloquently put by Ben Laurence:

> Chief Executives are usually sacked for one of two reasons. Some are kicked out because they have a perfectly sensible corporate strategy, but simply failed to implement it . . . And some are kicked out because their strategy is bonkers, and investors eventually realise it . . . Occasionally, just occasionally we come across a rare bird – a chief executive who can be said to have failed by just about any measure you care to mention. He (or indeed she) decides to pursue an absurd corporate dream. And even the pursuit of that dream is badly executed.[1]

Note that all references to IIA definitions, code of ethics, IIA attribute and performance standards, practice advisories and practice guides relate to the IPPF prepared by the IIA in 2009. With this in mind, we cover the following aspects of getting to a suitable audit strategy in this chapter:

8.1 Risk-based Strategic Planning
8.2 Resourcing the Strategy
8.3 Managing Performance
8.4 Dealing with Typical Problems
8.5 The Audit Manual
8.6 Delegating Audit Work
8.7 Audit Information Systems
8.8 Establishing a New Internal Audit Shop
8.9 The Outsourcing Approach
8.10 The Audit Planning Process
8.11 New Developments
Summary and Conclusions
Assignments and Multi-choice Questions

8.1 Risk-based Strategic Planning

There are many reasons why a CAE would want to develop a formal audit strategy and the benefits of a strategy focus have been described by one writer as follows:

> A strategy focus by the internal auditor can have many benefits some of which include being able to:
>
> - provide both those managing and evaluating performance assurance that the 'right things' are being done and done right;
> - assist those managing understand the need for synthesis of future external opportunities as well as analysis of internal problems based on extrapolating of the past; recognising and taking risk through innovation as well as minimising risk and maintaining stability;
> - recognise risk where it occurs and the four way communication necessary for the adaptation to changing risks and making them acceptable;
> - enable recognition as a learning organisation through the necessary use of the skills, knowledge and attitude of those managing; and
> - establish a clearly identifiable, understandable and acceptable basis for the scope of any audit.
>
> Adoption of a strategy focus will not only bridge the expectation gap but demonstrate that we are capable of responding to the increasing change in providing value to the organisation as it adapts also.[2]

Deciding clear objectives is the starting place for internal audit strategies. Directing resources towards accepted objectives sets the frame for success. The factors that impact on the process of setting clear audit objectives are noted in Figure 8.1.

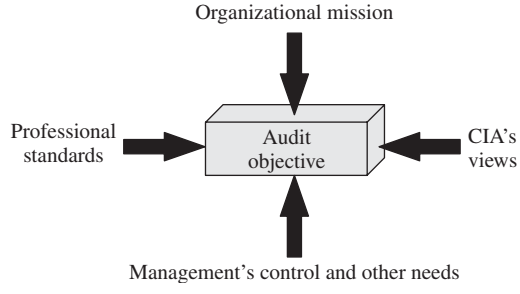


FIGURE 8.1 Setting audit objectives.

There is no one way of defining audit objectives as they result from the changing influences of competing forces.

Clear Objectives

This sounds straightforward but clarity of objectives is not always present. A basic test is to ask each auditor what he/she sees as his/her main objective. It is not enough to compose a formal document entitled 'audit objectives'. There is also a need for a clear but simple mission for the audit function, which should guide the entire staff. The variety of audit services is not a problem so long as an appropriate model is defined and applied. A real-life example follows:

A small internal audit section in a large private sector manufacturing company consisted of three staff. As a result of restructuring, a new manager was transferred from the sales department to head internal audit. On arrival he promptly announced he was unhappy with the dated term 'internal audit' and was changing the name to 'financial management'.

Scope of Audit Work

There is a need to decide what is included within the scope of audit work. It is possible to provide services outside the formal scope so long as we make a conscious decision. The scope of internal audit should be based on a professional framework. IIA standards suggest that the main role of internal audit is assurance work. Anything else is consultancy services which should be assessed through an appropriate criteria in line with IIA Performance Standard 2010.C1, which states that:

> The chief audit executive should consider accepting proposed consulting engagements based on the engagement's potential to improve management of risks, add value, and improve the organization's operations. Accepted engagements must be included in the plan.

A discussion of scope creates an opportunity to agree on the important distinction between audit's role in contrast to that of the management. There are various forces that impact on the final model adopted. These range from the CAE's views, the needs of management and the type of staff employed.

1. Communicated There is little point setting formal objectives for the audit function if these are not properly publicized across the organization. Communication may take the following forms:

- objectives embodied within an audit charter;
- suitable correspondence that repeats the objective;
- the annual audit report;
- regular meetings with management on this topic;
- formal presentations to the audit committee;
- some mention within major audit reports.

This is a continual process as strategy does not arise as a one-off event but changes and adjusts over time, in response to the environment.

2. Understood by all Passing formal documents out to auditors and management is not enough. There is a need to ensure that auditors understand and work to agreed objectives. For audit staff this may involve internally organized induction training and skills workshops. We may make a formal presentation to senior management that might be used to dispel myths and misunderstanding. It is essential that members of the audit committee have a clear understanding. Dave Richards who runs the First Energy internal audit team has spent time developing a clear mission and vision based around the team's:

1. products and services.
2. who are our customers.
3. what services do they use.

4. which customers are most supportive.
5. what does our feedback survey say.

The First Energy mission is that 'the IA dept. is responsible for supporting improvement to corporate performance, ensuring compliance with laws and procedures and confirming accuracy of corporate records'. Their vision runs along the lines of 'We deliver objective and innovative solutions.' This is built into their audit strategies and the staff competencies needed to achieve this vision are defined. They make the crucial point that the audit department is really the sum of the behaviours of its individual members.[3]

3. Types of services required The scope of internal audit sets a clear frame within which audit may operate. This will be designed to be widely applicable to most types of audit activities. The adopted scope of internal auditing can determine which services fall within the audit role. Those services that come under the audit head may be categorized. We can select an overall range within which services would fall within the remit of Figure 8.2.

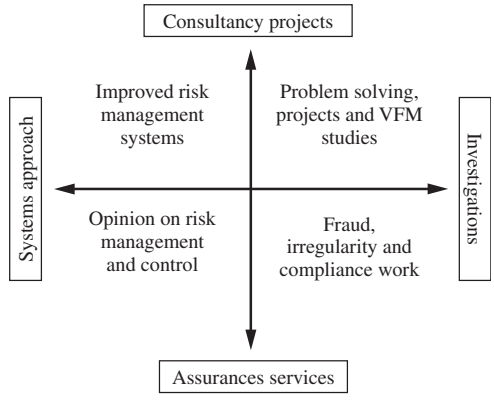


FIGURE 8.2 Types of audit service.

These four scenarios represent different areas for review available to audit management. It does not matter which model is chosen as this depends on how best audit resources might be applied, which depends on organizational needs. It is more important for audit management to plan and decide the type of services, armed with a good understanding of alternatives. Tackling new operational areas can pose a challenge for the audit team and a 10-point plan of advice has been provided on entering into uncharted waters:

> Audit staffs often face reviews of completely new or unfamiliar areas. While some audit departments shy away from such challenges, the internal audit staff at Sun Life of Canada charged full speed ahead with its audits of insurance sales and marketing practices – and reaped a bounty of rewards in return . . . Several tips for auditing a new area can be extrapolated from Sun Life's expedition into uncharted territory:
>
> 1. Think of the audit in terms of the benefits to the auditee.
> 2. Consider management as your customer.
> 3. Admit you need to learn more about the business, and then do it.
> 4. Solicit input from management regarding the risks and issues to review.
> 5. Take advantage of internal networks to facilitate the review.

6. Perform as much work as possible before going on-site.
7. Work with the auditee.
8. Choose the right people for the audit team.
9. Organize on-site visits to save you – and the auditee – time and money.
10. Recognize that one size does not fit all when it comes to reporting.

> . . . by thinking creatively, staying in tune with our customers' needs, and achieving consensus on the issues, we were able to be a positive agent for change in the organization.[4]

4. Policy on fraud work The topic of fraud holds a special place when discussing audit objectives. Auditors understand the control cycle that dictates that fraud is caused by poor controls. This does not detract from the need to set out our role in relation to fraud detection and investigation. The CAE must not only ensure that the audit role in frauds against the organization is documented, but also that audit is in a position to discharge this role. It is better to place a caveat by stating that the organization should provide additional resources for large projects. Management is ultimately responsible for investigating frauds.

5. Geared into the organization Any audit objective must be linked directly into the organization's own objectives (or mission). The starting place for setting audit's role is to isolate what the organization is trying to achieve and then see how audit resources can assist this. As long as we accept that our role is located in risk management and control issues, the final audit product may take different guises in addressing control-related matters. Risk management must be set within the culture of the organization and its success criteria. Organizations range between tightly bureaucratic entities through to loosely based project teams. The growth in non-traditional audit services may be geared to the way the corporate control environment has developed. Mike Summerell has given his opinion on moving away from traditional audit approaches:

> In my experience, traditional auditing tends to focus on formal accounting control mechanisms such as signature approvals, reconciliations, and documentation manuals. The results of these audits often focus on areas considered insignificant or 'bureaucratic' by staff and management. This view reflects another deficiency of the traditional approach – its tendency to focus on symptoms instead of the real causes . . . Auditors need to look for ways to enhance the services they provide. The CSA approach is not perfect, but it represents distinct advantages that more conventional approaches alone cannot offer. If the tried and trusted traditional audit techniques remain your sole approach to internal auditing, you are missing important opportunities. I firmly believe that traditional auditing simply doesn't have the potential impact of CSA. If, as a profession, we seize tradition as some virtue to maintain and champion, we may be flirting with extinction.[5]

6. Approved Any audit objective must be approved by the organization. This, in most cases, will be the audit committee where a formally signed audit charter will be agreed along with any changes.

Defining Audit Strategy

Strategy goes far beyond the old-fashioned annual planning updates that are described in *Brink's Modern Internal Auditing*:

> The director of internal audit today cannot develop an audit plan based solely on such factors as last year's plan and current available resources, publish the plan and proceed with audit activities.

> Many factors impact the type of audit activities that should be planned, and various functions and individuals within the modern organization will have some input into that planning process.[6]

The audit strategy process is a continuing cycle of events that must be properly controlled by audit management. The context is illustrated in Figure 8.3.

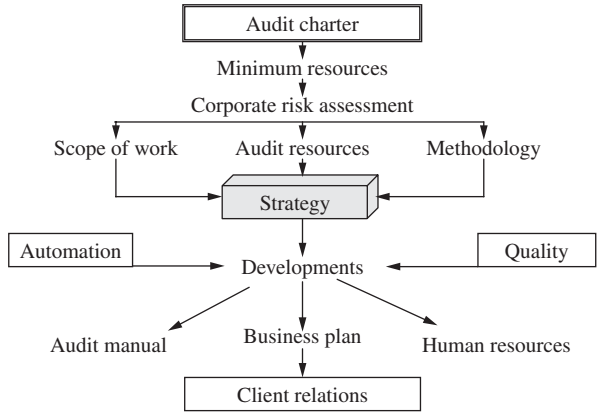


FIGURE 8.3 Establishing an audit strategy (1).

This diagram highlights the link between the audit charter, the organization's control need (as isolated through the corporate risk assessment) and the resultant strategy. This strategy helps determine what needs to be done (scope), by whom (resources), and how (methodology). It is then possible to set standards for the key issues of audit automation, quality assurance (QA), human resource management (HRM) policies and the audit manual. A confidential business plan would accompany the published strategy. The above may be addressed when formulating an audit strategy. An alternative strategic process is shown in Figure 8.4.

Here we seek to isolate gaps in the resources and procedures that we employ and address these gaps in the strategic plan.

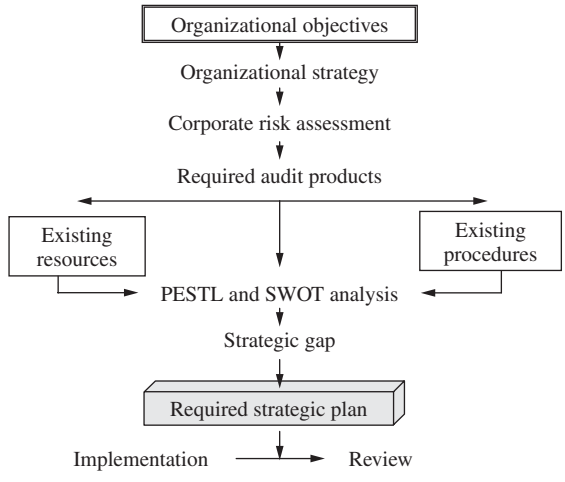


FIGURE 8.4 Establishing an audit strategy (2).

The Corporate Risk Strategy

A cornerstone of audit strategy is the corporate assessment of business risk. This establishes an organization's control needs. It involves the ongoing task of capturing the key systems that underpin an organization so that material control needs may be isolated and addressed. While audit objectives set out what we wish to achieve, control needs dictate how much work needs doing and the type of resources most appropriate. A risk survey necessitates discussion with middle management and involves:

- a definition of the audit unit;
- an assessment of the relative risks inherent in each unit;
- research into the type of problems units attract;
- risk ranking related to resources subsequently assigned via an audit plan.

1. Risk assessment We should construct a methodology that caters for different activities being associated with different types and levels of risk. IIA Performance Standard 2010 makes it clear that: 'The chief audit executive must establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organization's goals.' There is no universal formula but we need to ensure that:

- the methodology is accepted by the organization;
- it is applied to the audit universe in a consistent fashion;
- it is based on the corporate risk assessment and ongoing operational risk reviews.

The organization would have to be broken down into auditable units and one approach in *Brink's Modern Internal Auditing* suggests three options for identifying audit units:

1. by function – accounting, purchasing payroll.
2. by transaction cycle – cash receipts, production.
3. by geography.[7]

2. Management participation A further aspect of audit strategy relates to the need to involve management in the process. There is a temptation to become trapped inside the struggle to preserve audit independence, wherein contact with the outside world is avoided. Our plans and strategies are then based entirely on audit's perception of organizational needs on a 'we know best' basis. What may have been acceptable in the past can no longer be defended when all expenditure (including audit costs) must be justified to front line managers whose budgets bear the eventual recharges. Management participation is alluded to in IIA Performance Standard 2010.A1 which states that:

> The internal audit activity's plan of engagements must be based on a documented risk assessment, undertaken at least annually. The input of senior management and the board must be considered in this process.

There is a need to explain the audit process and demonstrate why resources should be directed at one area as opposed to another. Bringing management into the process means additional pressure on audit management. This derives from the need to perform one's job while at the same time communicating what is being done. A strategy not based on organizational needs and supported throughout the organization will be hard to implement. Management participation includes:

- explaining that audit operates to a risk-based strategy;
- ensuring that this strategy is based primarily on addressing organizational risk and control needs;
- publicizing the link between risk and resource allocation;
- keeping management informed as to changes to the existing strategies;
- securing avenues whereby relevant information may be imparted to and from management;
- clarifying the agreed cut-off points between management and internal audit's roles;
- retaining a degree of independence that gives audit the final say in strategy and planning.

PESTL and SWOT Analysis

Audit management is like any other management process in that all relevant techniques should be applied in the course of developing a clear strategy. Two such techniques are PESTL (an assessment of political, economical, social, technical and legal factors) and SWOT (consideration of strengths, weaknesses, opportunities and threats). These assist audit management in determining the current relative position of the audit function, along with some of the forces that may influence its future progress. The factors that might be pertinent to internal audit are:

Political The factors relating to government policy might affect the audit function. The government may turn towards internal audit as a safeguard against financial impropriety particularly where large-scale scandals receive press coverage. Where government policy calls for quality control over public services or controls over executive directors for enhanced corporate governance in the private sector audit implications have to be considered.

Economic Economic factors will affect the development of the organization, and might lead to growth, retrenchment or a basic maintenance strategy that should affect the audit style. Growth calls for expansion and aggressive policies with audit advising on the risk and control aspects of take-overs and new systems. Rationalizing may require closing down parts of the organization's activities and audit recommendations involving extra resources may not be appropriate. Economic factors may affect the audit budget and the supply of new auditors. Audit will consider whether a growth, retrenchment, or maintenance strategy should be pursued in internal audit.

Social Social factors must be recognized since they affect the culture of the organization. These include moral aspects relating to business ethics and wider issues like environmental protection. The rate of unemployment and supply of auditors should be appreciated along with the availability of training schemes. National opinion on fraud, VFM, accountability and business practices affect the role of audit.

Technology New technology has a dual role for internal audit for it will affect systems and processes used by the organization, and also expand the range of IT available for use in audit work. Audit strategy must keep up with IT developments and if possible stay a step ahead particularly in automating audit work. It is important that audit's IT strategy flows from that adopted by the organization.

Legal Audit must always keep up to date with legislation not only relating to the audit function itself but also legislation that requires compliance-based controls. Examples are health and safety, data protection, employee protection, equal opportunities, environmental issues, and accounting practices.

Strengths The positive factors may be developed and used to defend against threats and to seize opportunities. Strong features may relate to the quality of staff, degree of automation, special skills, a clear methodology and good client relationships.

Weaknesses Areas that need attention might jeopardize the welfare of audit. It is vital that these are identified and dealt with via the strategy. Common problems are:

Excessive non-recoverable hours	Low staff morale
Lack of audit procedures	Out-of-date audit manual
High staff turnover	Poor client relationships
Low-level audit work	Recommendations ignored
Poor quality of work	Assignments overrunning budget
No career development	Poor reputation

Each of the above problems must be addressed or the audit function will fail to fulfil its full potential. It is through a carefully planned integrated audit strategy that weaknesses may be tackled.

Opportunities The audit function should seize opportunities. Failure may cause the downfall of the audit department in total terms or in the level of the respect that it attracts. If the organization requires new services that might be provided through the audit function, it is important that this issue is considered. If there is a gap in controls in developing new computerized information systems and audit are unable to respond to this problem, the organization will find this expertise from elsewhere. If opportunities are not seized, they may pose threats in the future. The audit strategy should ensure that required strengths are developed to maximize available opportunities.

Threats Threats can come in many guises and may affect the status of the audit function. The obvious threats come as competition, and this can arise on many fronts including external audit, management consultants, and internal control teams. Developments within the organization may affect the level of independence acquired by audit and these must be countered. If the existing audit reporting line is stifling audit findings and recommendations, moves to find a direct link to the organization's power base through, say, an audit committee may be part of the strategy. If audit state their intention to perform high-level audit work, they must also have an additional strategy to ensure that their staff and procedures are sufficient to meet these new demands. A SWOT analysis may be used to address these factors as shown in Figure 8.5.

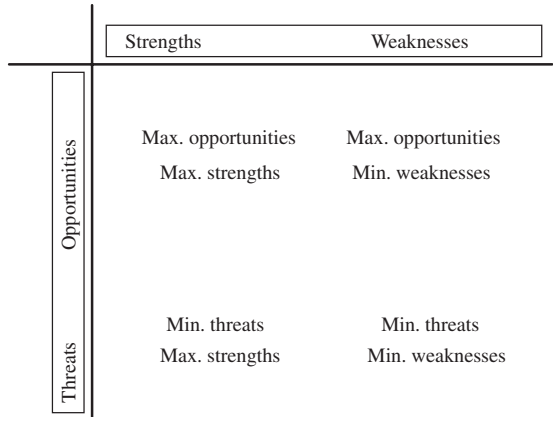


FIGURE 8.5 Illustration of the SWOT analysis.

Features of Audit Strategy

The bottom line in audit strategy is to assign resources to key areas. A parallel issue is whether the existing resources are sufficient to drive the required strategy. There exists an option to apply a 'push-or-pull' formula where strategy is either determined by the existing resources, or vice versa (Figure 8.6).

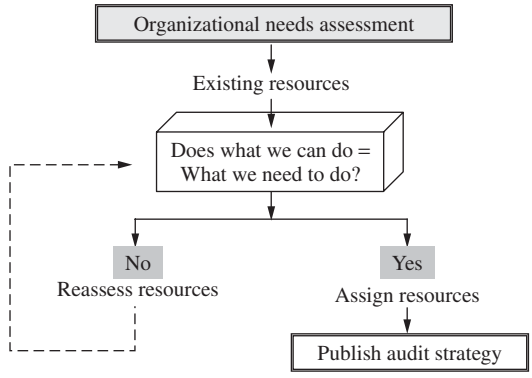


FIGURE 8.6 Audit resource application.

The key question is: Are we trying to do too much? The answer depends on:

- the profile of audit;
- the financial constraints and types of risks facing the organization;
- the procedure for approving additional bids against the revenue budget;
- the perceived importance of organizational risk and control issues;
- the level of support that audit have from line management and the organization generally.

The above process is a continuing one that should seek to constantly reassess audit resources in support of the desired strategy. There really needs to be a clear link between the risks facing an organization and the audit plans to cover the organization. Extracts from the IIA Practice Advisory 2010–1 make clear the linkage between the audit plan and risk exposures:

1. In developing the internal audit activity's audit plan, many chief audit executives (CAEs) find it useful to first develop or update the audit universe. The audit universe is a list of all the possible audits that could be performed. The CAE may obtain input on the audit universe from senior management and the board.
2. The audit universe can include components from the organization's strategic plan. By incorporating components of the organization's strategic plan, the audit universe will consider and reflect the overall business' objectives. Strategic plans also likely reflect the organization's attitude toward risk and the degree of difficulty to achieving planned objectives. The audit universe will normally be influenced by the results of the risk management process. The organization's strategic plan considers the environment in which the organization operates. These same environmental factors would likely impact the audit universe and assessment of relative risk.

3. The CAE prepares the internal audit activity's audit plan based on the audit universe, input from senior management and the board, and an assessment of risk and exposures affecting the organization. Key audit objectives are usually to provide senior management and the board with assurance and information to help them accomplish the organization's objectives, including an assessment of the effectiveness of management's risk management activities.
4. The audit universe and related audit plan are updated to reflect changes in management direction, objectives, emphasis, and focus. It is advisable to assess the audit universe on at least an annual basis to reflect the most current strategies and direction of the organization. In some situations, audit plans may need to be updated more frequently (e.g., quarterly) in response to changes in the organization's business, operations, programs, systems, and controls.

Audit work schedules are based on, among other factors, an assessment of risk and exposures. Prioritizing is needed to make decisions for applying resources. A variety of risk models exist to assist the CAE. Most risk models use risk factors such as impact, likelihood, materiality, asset liquidity, management competence, quality of and adherence to internal controls, degree of change or stability, timing and results of last audit engagement, complexity and employee and government relations.

Strategy is about keeping pace with developments to assume an advantageous position by anticipating and catering for the changes that occur naturally (Figure 8.7).

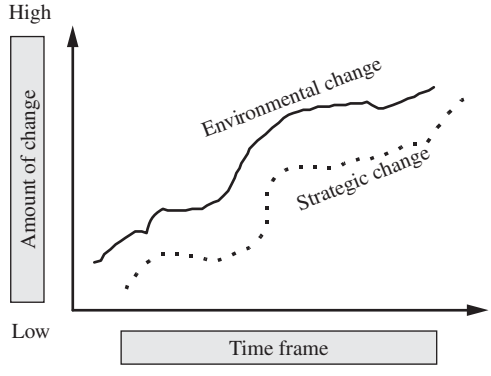


FIGURE 8.7 Strategic and environmental change.

1. Achievable The audit strategy must be realistic. It is possible to set high goals that motivated people may achieve. It is not business-like to produce plans that cannot be executed. The result will be the relegation of such documents to the wastepaper basket, or to an obscure file that is never looked at. Early successes in achieving adopted strategies have an inspirational impact on the audit team. If we are currently training IS auditors, this takes time. It would be inappropriate to suggest that fully equipped IS auditors would be on-line in a short period. There is a temptation for audit management, led by a distanced CAE, to develop a whole set of strategies and plans not discussed with staff which are unrealistic. There is a fundamental imbalance in the equation:

Does what we can do = What we need to do?

It is incumbent on the CAE to reconcile this equation and not only promise a great deal but also ensure that what is promised is subsequently delivered.

2. Implemented If an employee starts work in a new department and wishes to enquire into the strategy that management have adopted to develop and run the department, he or she may ask one question:

> Am I aware of any particular strategy?

If the answer is no, then enquire no further. We cannot have a strategy without communicating this to all those who are expected to discharge it. This basic point is overlooked by many managers who see the strategic process as a form of undercover operation. The confusion comes about because some aspects of a strategy are confidential to outsiders. This may relate to unit costs of the services provided or how competition will be tackled, or how audit might seek to take over various associated functions such as quality assurance. These issues may be dealt with via a confidential business plan. This does not mean that the staff within the audit department are not advised. We may involve all auditors in the strategic process. They must not only be sold to the ideas but should also help produce them by the practice of active involvement. Group meetings, regular consultation, and vibrant discussion sessions all help to establish this principle. Away days and seminars held at suitable hotels, away from work, help produce this sense of involvement. Meanwhile, the audit strategy should also be communicated to the board and audit committee for approval and meet the requirements of IIA Performance Standard 2020 which states that:

> The chief audit executive must communicate the internal audit activity's plans and resource requirements, including significant interim changes, to senior management and the board for review and approval. The chief audit executive must also communicate the impact of resource limitations.

Once a strategy has been approved, we need to ensure that objectives cascade downwards as a component of implementing strategy as illustrated in Figure 8.8.

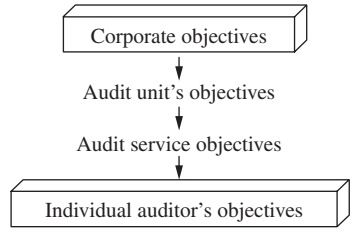


FIGURE 8.8 Cascading objectives.

3. Long-term plans The link between audit strategy and audit planning is shown in Figure 8.9.

Whatever audit strategy seeks to achieve must be secondary to the resulting formal audit plans that are produced as a result. These plans set out the audits that will be performed over a defined period that constitutes the substantive work of the audit function. The strategic process allows these plans to be prepared through a mechanism derived from best management practice. We cannot move straight into the planning process without first setting the correct context by applying formal strategies. In fact the IIA Practice Advisory 2020–1 states that:

> The chief audit executive (CAE) will submit annually to senior management and the board for review and approval a summary of the internal audit plan, work schedule, staffing plan, and

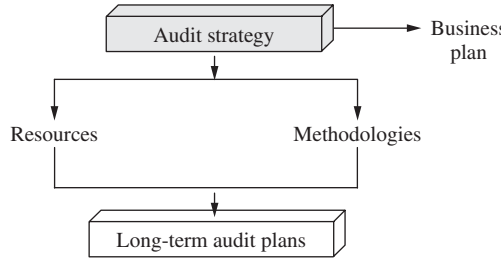


FIGURE 8.9 Strategy and long-term plans.

financial budget. This summary will inform senior management and the board of the scope of internal audit work and of any limitations placed on that scope. The CAE will also submit all significant interim changes for approval and information.

The CAE should submit annually to senior management for approval, and the board for its information, a summary of the internal audit activity's work schedule, staffing plan, and financial budget . . . the board should be able to ascertain whether the internal audit activity's plans support those of the organization.

4. Preliminary surveys How much detail should long-term plans provide? Risk assessment allows one to judge which areas should be subject to audit cover. This feeds into the strategic process and, along with other things, results in a long-term plan of work that will help direct the activities of the audit function. The question then arises as to how an audit can be picked up from these plans and performed without a great deal of additional effort. We may feel pressured into conceding that long-term planning must establish formal terms of reference for these planned audits. Fortunately, the preliminary survey comes to the rescue since we need not provide detailed plans for each audit over and above the act of selecting those areas that attract a high level of risk. The preliminary survey allows us to take an audit area and carry out some background work with a view to setting formal terms of reference for the ensuing audit. We have shown that audit strategy must operate at the highest possible conceptual level over and above the day-to-day workload of individual auditors. The preliminary survey helps interface the resulting audit field work with these generalized issues.

5. Contingency allowances It is sensible to set aside resources for matters outside the general work of the audit function. There are emergencies and unexpected events that call for change in strategy or short-term additional resources, which must be accommodated by audit management. Audit strategy should not only assign resources to audit work but must also allow resources to deal with unforeseeable problems. There are two ways to avoid installing large contingency allowances into strategic resource planning:

- Provide a mechanism whereby additional short-term resources may be taken on and dropped at short notice. Internally funded project teams, external consultants, agency staff and staff employed on fixed-term contracts can all be used to secure these additional resources as and when required. The secret is to be able to shed these extra resources at short notice, once the project/problem has been completed/resolved.
- Construct a strategic process that operates on a short-term basis and is subject to continual and constant review. Where this is implemented we would be in a state of constant change, where resources were continually changing to meet new demands on the audit function. This

approach is high risk, and must be closely controlled by audit management. One might imagine monthly audit manager meetings driven by the CAE, where resources are switched, secured and terminated at short notice. This will tend to have an unsettling effect on staff and the constant change will not promote much personal development or consistency. In times of recession and major change, it can be used to keep in touch with the fluctuating demands on the audit service.

Best practice audit shops were considered by the IIA in their guidance on implementing the professional practices framework. In terms of planning flexibility they found that:

> Many organizations are building flexibility into their audit plan, so that they can address risks as they arise throughout the year. Audit shops may leave 30 percent to 40 percent of their time unallocated, for example. Others may commit to spending a certain amount of time to a functional area but stop short of identifying specific projects. When the time arrives to perform one of these conditional engagements, the auditor spends 10 to 12 hours preparing a business plan for the project that is submitted to audit management.[8]

Successful Strategic Implementation

Strategic development is getting auditors to work together proactively to drive the audit service forward in the right direction. The need to rally round a clear goal is fundamental to the success of any strategy. A chain may be established by the CAE that represents the flow required for successful strategic implementation as in Figure 8.10.

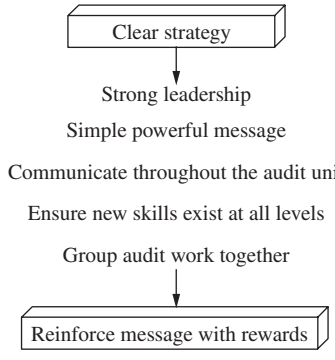


FIGURE 8.10 Successful strategic flow.

This is an important factor for audit management to acknowledge since it is based on strong leadership that drives a powerful message throughout the audit function. Barry S. Leithhead has suggested seven strategies to help internal auditors ensure that their communications with senior management yield mutual understanding as well as approaches to risk management that best serve the needs and goals of the organization:

1. Enlist the support of senior management for internal auditing's risk-based approach and objectives. Think of risk from management's perspective rather than just focusing on audit-related concerns.

2. Adopt a relevant language to develop understanding about risk. A risk glossary should include – risk sources, risk causes, values at risk, consequence, likelihood, control.
3. Facilitate a risk assessment workshop to identify significant exposures.
4. Discuss the priorities for the annual audit plan. Respond to key risks.
5. Contribute to the strategic planning process.
6. Periodically inform senior management about emerging priorities. A risk watch forum.
7. Regularly inform senior management about high risk areas when reporting the results of audit projects. Red, green and amber ratings may appear on reports that also explain links to key performance indicators.

Regular and effective communication with senior management can help to ensure that risks are understood and that controls are designed to adequately address existing exposures, with the flexibility to anticipate future risks.[9]

Setting Long-Term Goals For Internal Audit

By Dan Swanson, *Compliance Week Columnist*

Internal audit efforts must be risk-based and contribute to the long-term assurance needs of the organization and its board. A formal risk-assessment audit must be completed at least annually and the results of that assessment should direct audit priorities. Over the past five years, a focus on short-term results (quarterly financial results and meeting current regulatory requirements) has driven the priorities of management and consequently the organization toward a short-term perspective. Similarly, internal auditing's efforts have moved toward this short-term focus, boiling down priorities to whichever audits the company needs to complete in the immediate quarter. The turn of the calendar year is an excellent time to refocus sights on the long-term horizon. For example, what does the organization want to achieve in the next three to five years, and what does it need to do to get there? Certainly, each organization will have different goals, objectives, issues, and challenges, and no single ''standard'' long-term internal audit plan will work; but I took a shot at it anyway, and present the results below.

The Top 12 Internal Audit Priorities

Over the next three to five years, internal audit departments should evaluate their organizations' efforts in the following areas and provide their ''opinions'' to management and the board.

1. **The enterprise risk-management program.** To my thinking, ERM is a silver bullet for improving governance and organizational results because it identifies your key objectives – and managing risks that accompany those objectives is effective governance. Whether your organization is a proponent of COSO's risk-management framework; the Australian risk-management standard; the governance, risk, and compliance guidelines from the Open Compliance and Ethics Group; or other standards, it is time for organizations to take ERM to the next level. Completing an internal audit of the organization's ERM efforts will provide everyone with a baseline assessment report that also will reveals gaps in risk management.

2. **The top three most significant business initiatives.** Over the past 15 years I have promoted (indeed, strongly encouraged) the auditing of the top three most significant IT initiatives. This year and going forward, I now firmly believe in auditing the three most significant business initiatives, with a very robust analysis of the IT component for each of these initiatives.
3. **The business-continuity program and the disaster-recovery program.** BCP and DRP are on everyone's list of top 10 priorities; the problem is that they always rank in the bottom half. It is now time to ensure that the organization's resiliency efforts are truly operational. Establishing a robust preparedness capability is also one of the best investments an organization can make; auditing BCP and DRP efforts will assist the organization greatly in ensuring that the proper attention is given. An effective business-continuity capability is absolutely essential, although being able to recover IT is of course critical.
4. **The information-security program efforts.** Protection of an organization's assets is a critical activity; for some companies it is the most critical activity. Auditing an information-security program is also a long-term effort involving many audits over many years, and it is time to start that long-term assurance effort. A very simple starting test: Has the effectiveness of your security efforts been discussed at the board level this year?
5. **The overall governance regime.** Corporate governance; organizational governance; performance accountability; governance, risk, and compliance – governance goes by many names. Internal auditing provides assurances to management and the board regarding an organization's governance, risk-management, and controls processes. Therefore, fundamentally, internal audit should provide an opinion regarding the overall governance ''regime,'' regardless of the exact term your company uses to describe its efforts. Sustainable development and corporate social responsibility issues also should be considered.
6. **The compliance and ethics program efforts.** Compliance and ethics efforts have received enormous attention (and funding) in the last five years, and this will continue over the next five years. Depending on the internal audit department's past efforts, audits of the compliance and ethics programs should either drill down into specific opportunities or become much more high-level to provide an overall assessment.
7. **Records management.** Some people may disagree with including this item on my list or ranking it so highly. My point for including it is that if your organization has not started upgrading its records-management program to reflect today's regulatory requirements and technological capabilities, then the organization is 'at risk.' An audit of the records-management program will assist in the determination of what opportunities for improvement do exist. There is nothing worse than having a policy and not following it.
8. **The quality of the enterprise information for decision making.** Information is critical to every organizational effort. The quality of the organization's information will directly affect organizational results and, therefore, should be assessed on a regular basis – by management and by internal audit. Information management will become more critical every year.
9. **The anti-fraud program.** Sarbanes-Oxley (and equivalent governance-related legislation elsewhere) was passed to reduce the occurrence and impact

of fraud and to increase the reliability and integrity of financial statements and related management assertions. Anti-fraud programs need to be established (or strengthened) as a result of these new governance requirements. The board and management need to know that these programs work effectively.

10. **The IT function's efforts to meet business needs.** This audit priority is extremely diverse. The IT function performs a broad range of services and it has a substantial impact on business results. As a result, the IT audit priorities require a more detailed risk assessment to determine what the audit priorities should be. Fundamentally, evaluating the IT function's efforts to meet business needs is a core audit requirement. Assessing IT's effectiveness, efficiency, and ''customer service'' are the three main components of an effective IT shop. Deciding on further IT audit ''focus'' beyond these areas needs to be based on a more formal IT risk-assessment audit.
11. **Board and executive management service requests (consulting and assurance projects)** This audit activity is an important catch-all to assist with the specific or unique needs of the organization. It is also included in my top dozen to highlight the need for a customer service ''philosophy'' by the internal audit function. The percentage of the audit budget allocated to this important activity will differ widely, but it lets the board and management know that internal audit is responsive to the board's assurance and consulting needs. Of course, these ''special'' audit projects should be of significant value to the organization, and they should not distract from the delivery of the overall audit commitment.
12. **Process management, including continuous process improvement.** My last audit priority relates to improving organizational performance. I label the audit priority ''process management'';

Your company might call it a Six Sigma program, while others might call it a corporate quality-management initiative. This audit priority is focused on encouraging and confirming that there is an organization process-improvement program in place, whatever the title. If the organization has not established an organizational program to improve its performance on a sustainable basis, it is at risk.

Defining The Long-Term

As I mentioned previously, each organization is different, and its internal audit priorities will be different, too. Still, for any organization, internal audit's priorities should be risk-based and should focus on the organization's governance, risk-management, and control processes. Corporate-wide ''themes'' of cost efficiency, cost effectiveness, strategic management and control, quality management, process improvement, and so forth will (and should) influence your internal audit efforts over coming years. You also should ensure that the internal audit plan has a strong linkage with the organization's strategic plan. The bottom line: It is time for executives to lead, managers to manage, boards to govern, and auditors to provide assurances to the board and management that things are as people say they are. Your next audit-planning effort should make this clear – to everyone.

Reprinted from *Compliance Week*. This article was originally published in Compliance Week. Reproduced by permission of Compliance Week. All rights reserved.

8.2 Resourcing the Strategy

Resource management and human resource management (HRM) are major components of the strategic management process. The IIA Performance Standard 2030 makes it clear that:

> The chief audit executive must ensure that internal audit resources are appropriate, sufficient, and effectively deployed to achieve the approved plan.

We include here the main issues that impact on HRM within the context of internal auditing.

Management's Role

Audit management must ensure that HRM issues are adequately considered and dealt with. This sets the stage for defining management's role as one of managing (not performing) the audit work in larger audit shops. There are potential complications, since managers may find it hard to stop auditing and start managing. The fact that the type of work that auditors tend to handle can be very sensitive provides a convenient excuse for audit managers not to refer the work down to their staff. The position we need to reach is where audit managers appreciate the need to employ staff whom they can trust and rely on to discharge the audit role. They need to ensure that the staff are properly developed and directed so that they are able to perform to accepted standards. The only way that this can be achieved is through the application of suitable HRM techniques. A further complication is that HRM matters must be set within the overall framework of the organization's own HRM policies. Audit management is restricted by the autonomy it has in the application of policies specific to internal audit. Having said this, everything that auditors do or fail to do is the direct responsibility of audit management and ultimately the CAE. IIA standard 2000 states that:

> The chief audit executive must effectively manage the internal audit activity to ensure it adds value to the organization.

The CAE is responsible for properly managing the internal audit activity so that it meets stakeholder expectations and conforms with the IIA IPPF.

Traditional Weaknesses in Management

Management may actually impose barriers to audit performance:

1. A failure to appreciate the principles of good HRM can undermine the whole audit department. We have the truism that it is only good managers who are able to apply good HRM policies. An old-fashioned CAE who is stuck in old ways will make little progress.
2. There is a temptation to refer all matters on HRM to the personnel department for them to deal with. This is a failing as it is only audit managers who really appreciate the audit role and what is needed by their staff to discharge it. Recruitment, selection, training, development, appraisals, discipline, and codes of conduct are matters that cannot simply be referred to personnel.
3. Progress can be made by enlightened management where new ways of developing staff are devised and motivation is managed professionally. Managers who perceive their staff as a problem are less likely to inspire excellent performance.

If audit management is not able to lead from the front, it will not inspire confidence:

> A chief audit executive spent much time reviewing reports produced by his senior auditors. He would ask for changes and alter the way a basic point was expressed, although the point remained the same. This was a drawn-out process suffered in silence by each group auditor. Over the years, this continued until the CAE prepared a short report on an audit he was personally involved in. This report was of poor quality and contained repetition and woolly terms. The group auditors got sight of it and lost confidence in the CAE whom they began to openly criticize.

The Human Resource Management Cycle

The audit plan must be properly resourced, which, for internal audit, mainly consists of getting in the human resources. This is required by IIA Practice Advisory 2030-1 which makes it clear that:

> The chief audit executive (CAE) is primarily responsible for the sufficiency and management of internal audit resources in a manner that ensures the fulfillment of internal audit's responsibilities, as detailed in the internal audit charter. This includes effective communication of resource needs and reporting of status to senior management and the board. Internal audit resources may include employees, external service providers, financial support, and technology-based audit techniques. Ensuring the adequacy of internal audit resources is ultimately a responsibility of the organization's senior management and board; the CAE should assist them in discharging this responsibility.

It is as well to define what we mean by HRM. Personnel issues are unrelated matters that concern staff, which are dealt with partly by personnel and partly by line management. These can relate to travel claims, overtime, sickness records, time sheets, timekeeping and so on. Their impact on the relationship of the employees and employer are but single issue topics. HRM, on the other hand, is concerned with a whole system of management that is designed so that the right people are doing the right things at the right time, to ensure organizational objectives are achieved as in Figure 8.11.

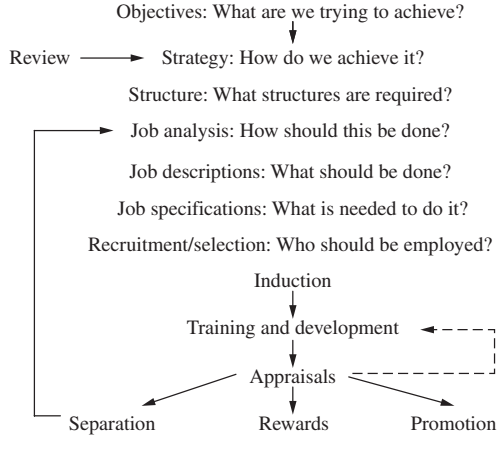


FIGURE 8.11 The human resource management cycle.

Attributes of Auditors

Auditors will be able to deliver quality services where the following hold true:

1. The objectives are clear.
2. What is expected of them is made clear.
3. The standards of performance are made clear.
4. They have the ability to perform to the requisite standards.
5. They are motivated to do so.
6. Management removes any barriers to performance.

There is an unstated assumption that the auditor has the right attributes to perform to the requisite standards. This can only arise where audit management has defined these attributes so that recruitment and development programmes can be directed towards them. If this definition has not been carried out then it becomes guesswork. At worst, auditors may guess wrongly and behave in an inappropriate way because this is what they assume is required. Internal audit competencies are also discussed in Chapter 5.

The Importance of Clear Personnel Policies

The CAE has a clear responsibility to install suitable arrangements for managing human resources and this is a feature of this section. However, these procedures must be set firmly within the context of the organization's personnel policies. There are two extremes that may be used to formulate a suitable model to deal with this as in Figure 8.12.



FIGURE 8.12 Autonomy versus compliance.

The CAE should try to move the department towards the right. Here audit managers become responsible for recruiting, training, developing, appraising, promoting, counselling, disciplining and dismissing their own staff. Where the organization has adopted good employer policies designed to create a balanced and stable workforce, the general principles should ideally be retained. It is advisable to use the personnel managers as consultants when considering changes to staffing. The role of the organization's personnel policies is important since the CAE must ensure that the internal audit department complies with relevant procedures. Divergence must either be allowed or specially approved by the organization.

The internal audit angle Internal audit should ensure that all HRM policies are clearly documented and made known to staff. The ideal vehicle for this is the audit manual where internal audit policies and procedures are considered, designed and detailed. We would look for clearly defined policies over a range of audit-related issues (and not just the ever-sensitive issue of auditors' expense claims). These would be general in nature and the CAE would then redefine them in greater detail to incorporate specific internal audit matters. An example follows:

The organizational policies on selection interviews state that each candidate will undergo a formal interview carried out by a suitably constituted panel which includes a personnel officer. The CAE then sets out an internal audit policy based on this which states that the panel will consist of the CAE, relevant audit manager and the personnel officer. Each candidate for an audit post will be required to undergo an hour-long written test based on an in-tray situation, which will be assessed before the formal interview is carried out. The interview will include questions concerning the submitted test paper.

Here organizational policies are complied with while specific audit-related matters are taken on board via more detailed procedures. This should be recorded in the audit manual. The onus is on the CAE to ensure that the audit shop is able to meet the requirements of Attribute Standard 1210, which means: 'Internal auditors should possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively should possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities.'

Recruitment Selection

In theory, the recruitment process starts with an HR planning exercise that seeks to identify which resources will be required and how they will be secured. We start with the analysis of a post that has fallen vacant. Job analysis involves the following procedures:

- The structuring process (following strategic analysis) will result in a number of defined roles within the internal audit function. An outline budget should have been approved to appoint personnel to these roles.
- These roles along with any vacated posts will be made available for job analysis which will assess the way a post will be defined in line with the required work duties.
- The type of work that is needed to discharge the defined roles will be assessed with respect to these funded positions. This is defined through a consideration of several matters including the funds available, whether the vacant post should actually be filled, the existing levels of expertise within the audit department and the changing needs of the audit unit (as captured through the strategic analysis).
- An outline statement of objectives will be defined that attaches to the vacant post. This will set out the job title of the post and a brief description of its role along with a view of reporting lines within the internal audit unit.

1. Job descriptions The next stage in the recruitment procedure is to formally define the requirements of the post. The process of setting the job description is one of considering the ensuing contract of employment that will be entered into by the incoming appointee. This process may be documented as:

1. Define the key responsibilities of the post having regard to other jobs in the section.
2. Include the main components that apply to all audit staff in line with the level of responsibility of the post.
3. Set out the categories of activities that will be required from this job in distinct groups such as:
   - managerial responsibilities

- internal audit responsibilities
- organizational responsibilities
- compliance with defined procedures
- compliance with relevant legislation
- compliance with professional code of conduct.

4. Write out a formal job description and ensure that it is consistent with the others across the audit department. Remember that we may wish to promote the use of generic grades where movement between auditors may be readily arranged to promote a flexible workforce and career development.
5. Carry out a formal job evaluation and assign an appropriate grade to the post that fits with the requirements as defined via the job description.

2. Job specification We can now define the type of person who would discharge the requirements of the job description. This is known as specifying the job. Not only will the final version provide a basis on which to select a suitable individual but it also has the key role of forming the foundation for any performance appraisal scheme. There are different ways that the specification may be achieved:

1. Establish the essential requirements for the postholder in terms of formal physical attributes, qualifications and years/levels of experience.
2. Establish the desirable requirements across a range of factors including managerial skills, supervisory skills, auditing skills, specialist skills, personal attributes, relevant experience over a range of audit-related areas and other material factors.
3. Review the specification to ensure that the needs of the job description would be fully catered for by the detailed skills that have been agreed upon.
4. Review the specification to ensure that it falls in line with other job specifications for other audit posts and complies with the spirit of personnel policies particularly relating to formal qualifications.

3. Recruitment Much of the above material falls under the recruitment procedures that precede the selection of actual staff. However, we must also address all the other pre-selection matters including:

1. The compilation of a suitable advertisement for the post. It is good practice to mention essential requirements from the job specification so as not to mislead applicants who may not realize that they will not qualify for the position. The advert is also a marketing device in that it may contain a public commentary on the audit department with well-chosen phrases such as 'a progressive department', 'a highly successful audit service', and 'in line with the highest professional standards'.
2. The selection of a suitable medium depending on the grade of auditor being appointed. It may be advisable to adopt the policy which states that the more senior the audit post, the greater the effort to find a suitable candidate. Thus audit managers and the CAE may be selected via a formal recruitment consultant while junior posts may simply be advertised in an appropriate journal/newspaper.
3. Arrange a package of pertinent material that should be made available to applicants. This will include the job description, job specification, material on the audit department and a brief background to the organization in question. Some provide the name of a person within the

audit department who can be contacted for an informal conversation concerning the vacant post. This is time consuming but can be useful in helping to vet potential applicants and ensure that applicants are really sure they wish to be considered for the post.

4. Define a convenient recruitment process that allows potential applicants to make contact, receive papers, submit an application and receive confirmation of receipt of their forms. Professional arrangements will add to the overall image of the organization/internal audit function.

4. Selection The final stage is to establish a formal selection panel for the entire process. This may consist of the CAE, an audit manager and a personnel officer who review the completed applications to shortlist for interview. The audit manager has managerial responsibility for the appointee. Shortlisting should be carried out by the selection panel soon after the advertised closing date. Applications may pass through a variety of stages depending on the number of responses (Figure 8.13).

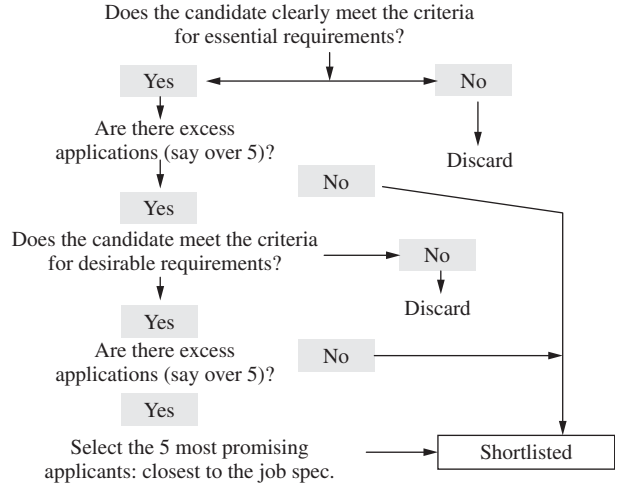


FIGURE 8.13 Job application shortlisting.

The maximum number (five in our example) should be decided beforehand. It is impracticable to interview dozens of people and then seek to select the best one as this leads to an information overload. The final decision on maximum numbers must fall in line with organizational policy. There is debate as to whether personal references should be secured at this stage. The application form may ask for the name and address of, say, two referees. If references are taken up beforehand, this may well delay the entire process and if they are persons nominated by the applicant, then they serve little real purpose in terms of providing an independent appraisal of the person concerned. The only useful reference is a questionnaire that is sent direct to the personnel department of the applicant's current or last employer. It is good practice to check professional qualifications as it is not unheard of for these to be falsified. There can be many anomalies in application forms. A candidate may claim to be a member of a professional body and it may be unclear whether this is by examination. There is an example of one application form which set out details of the various stages of an MBA that was studied at a particular university. Unfortunately, it was not made clear from this form that the person had withdrawn from the programme without completing it. Any

question marks over the reliability of personal data must be resolved when appointing auditors and the CAE must adopt the view that we can never be too careful.

There are professional interviewees who are very comfortable in what should be a highly pressurized situation. They give off a relaxed charm that can persuade the panel to appoint on the basis of the candidate being a very pleasant person. Good interpersonal skills are a very useful attribute but have little use if auditing skills have not been mastered. An extremely pertinent skill that may be tested as part of the selection process is that relating to report writing. Poor reporting skills are very hard to rectify, particularly where the auditor is on a senior grade. A way around this problem is to give each candidate a written piece of work ('test' is an emotive word) that should be completed, say, within an hour, and handed in to the selection panel before the interview is started. It is better to interview a small number of candidates and have extended interviews in contrast to meeting large numbers of hopefuls for a short time each. The candidate may be asked to present the work which would ideally be in a report format. This work will be assessed along with the performance in the interview as part of the decision process. An example helps:

> An auditor was appointed to fill a general audit post as a semi-senior. She did not have an audit background but was very enthusiastic at the interview. Furthermore, she had a good sense of humour and a very nice presentation. After several months, her manager realized that her report writing skills were very poor and not only did she fail her internal audit examinations several times but she found it impossible to draft a sensible report even after much training. She was eventually disciplined and dismissed as the result of an inability to perform to acceptable standards.

Note that some organizations use assessment centres to test various attributes of candidates before they are shortlisted. The main part of the selection process has traditionally been the formal interview. Although this technique has been much criticized, it would appear to be a most convenient way of getting to know the candidate and making a reasoned assessment of their potential ability. In fact, we can make two levels of assessment in an interview involving the understanding displayed by the candidate and second, the way he/she handles an interview situation. The latter point is related to the view that interviewing/communications skills is, in itself, an important attribute for the auditor. The interview format provides an opportunity to ask relevant questions and in this way test the candidate with a series of pre-planned questions. It is important to ensure that each interviewee gets the same questions and that they are directly linked to the job specification. It must be said that the interview also gives clues as to whether the person will 'fit in' with the audit shop, although most experts recommend pursuing diversity as a healthy goal. As a final point, the selection panel must ensure that there are no outstanding queries after the interview has been concluded. All relevant issues should be voiced even where they are sensitive.

There is one example on record of an auditor being appointed to a post when, unknown to the panel, he had already resigned from his current employer 'under a cloud'. The assessment process must, as far as possible, be applied in a consistent fashion to all the interviewees. There is only one question that the panel should ask and this must be: How far does this person meet the job specification? This must be the overriding factor. Note that a controversial candidate who has much initiative may create some conflict with the panel but this is not necessarily a bad thing. It is sometimes necessary to break the cosy world of internal audit where everyone agrees with each other, and seek to bring in some new ideas. A fresh appointment can promote this situation as

long as this new-found conflict can be managed by the CAE to provide a constructive debate to the overall benefit of the internal audit function.

Selection is the next stage where a suitable appointee is selected to fill the vacant post. The criteria for selecting the right auditor should be clearly set in the minds of the panel members. First, a selection should only be made if the best candidate is appointable. If this is not the case, the post should be readvertised and the previous applicants should not be invited to reapply. If there is more than one person suitable for the job, one must then go through a process of elimination that allows the person who most closely meets the job specification to be chosen. A point-scoring format may be applied that, while not being wholly scientific, does impart a level of consistency for the process. An alternative approach is to 'free-float' with open discussion of the key points so that a picture is painted rather than a points scale filled in. It is also possible to set each person off against the others and so seek to eliminate them one by one until a choice is made by default. Whatever be the approach, the CAE should ensure that there is a clear method through which such a selection may be made and that this is properly applied by the interview panel. The final point to note is that it is not always possible to contain the process of gathering information on the candidate within a set framework. Even where standard questions have been designed, there will always be a level of discussion that may lead into other related areas. A good interviewee may, in practice, gently lead the panel into topics that they are happy to discuss and which reflect well on them.

Most auditors find it comfortable working with checklists and procedures and this is how it should be. Once a selection has been made, it is a good idea to go through a formal checklist of matters that have to be dealt with before the appointee turns up for work. This checklist will cover important steps that must be taken such as references, start dates, probationary periods, payroll, new starter routines, medical examinations, contracts of employment, induction training, security passes, facilities such as laptops, etc. At some stage, and this should ideally have been done at shortlisting, the information contained on application forms should be verified including qualifications, past employment, residential status, etc. The formal contract of employment will have to be signed before the auditor is taken on. This may appear to be a formality at first sight but, in the event of a dispute, can be very important. For audit staff, there are several special matters that should be incorporated into the contract of employment. These provisions should cater for travelling and overnight stays, subsistence allowances, unsocial working hours, compliance with professional auditing standards/code of conduct, meeting time budgets and so on. As a word of warning, it is not unheard of to review a selection of personnel files and find that some of them do not contain signed contracts of employment.

Once the auditor is in post there should be a suitable introduction process. This is a matter of acclimatizing the newcomer to the audit department in terms of management's expectation of him/her. Induction is not only required for junior staff, it is useful for all grades who will benefit from an explanation of how the particular internal audit department operates. Some warning of expectations should be outlined in the selection interview since selection is about both offering a job and having that offer accepted by the candidate. Both sides must be satisfied with the arrangements before they are finalized. If the requirements of the audit manual are made clear to the candidates between the time of selection and signing the contract of employment, they will have a chance to withdraw if not happy with the procedures that are applied in the particular internal audit department. Induction should be based around the audit manual, although one would also cover the wider organization and any important policies that are in use. This induction could be on two levels. One may be a half-day consisting of general organizational matters on a one-to-one basis. A formal programme may be arranged for a batch of new auditors that may

last a full day and, as already mentioned, should consist of material taken from the audit manual. This may be presented by a senior audit manager.

The Career Development Profile

The world of internal audit is, in fact, fast moving and going through a process of continual change, generally to the advantage of the profession. One such development is related to the view that we may now have a career in internal audit. Not so long ago organizations felt it necessary, when advertising for audit staff, to promise a transfer to line management after a spell in internal audit. As such it was seen as good training in a function that potentially came into contact with all aspects of organizational activities. Good all-round general managers who had, as it were, a helicopter view of the organization, could in this way be developed. There are two main arguments located in this view of the audit function. First, the fact that internal audit provided a good training ground for managers is a valid concept. However, the perception that one must use bribes to encourage people to join internal audit, which is the second implication, is misguided. Furthermore, the management career development programmes that use secondments to internal audit can run hand-in-hand with separate programmes for career internal auditors. As long as audit careers are respected in their own right, there should be no problems. This section is based firmly on the concept of internal audit as a formal professional career.

8.3 Managing Performance

Staff appraisal is a management control that audit would tend to recommend when undertaking an audit where staffing is included in the terms of reference for the work. As such one may argue that we, as auditors, should apply this technique to the management of the internal audit function. However, staff appraisal schemes can be positive motivators or complete demotivators depending on how they are designed and implemented. The theory of staff appraisals is based on telling people what is expected of them and then telling them how far they are achieving these standards, as a way of motivating them. The other benefit is the positive steps that may be taken where performance is not on par. Appraisal schemes also underpin career development programmes that again may be used to direct the activities of staff and ensure there is good progression so that good staff are retained and poor staff improved. This may be illustrated in a simple diagram as in Figure 8.14.

An alternative approach to the appraisal process is to separate performance appraisal from procedures for dealing with unacceptable poor performance and particular problems. The latter would come into operation where there are obvious flaws in performance, which cannot be addressed through traditional training and development programmes. Figure 8.14 is based on the organization distinguishing between different management procedures for dealing with a variety of performance-related issues. As such where the auditor breaches procedure, this is dealt with through the disciplinary procedure. Where the employee is often sick, the frequent sickness procedure comes into action; and poor performance is handled by special action that may result in dismissal of the auditor in question. In this way, the performance appraisal scheme can be operated in a positive mode at all times. Special staffing problems are handled by distinct and separate arrangements outside performance appraisal. Special attention will be directed towards the auditor and this will not wait for or be dependent on the performance appraisal programme. In this way, these types of problems can be fast-tracked before they get out of hand. Meanwhile the appraisal scheme may continue in its positive mode. The words ‘performance’, ‘development’,

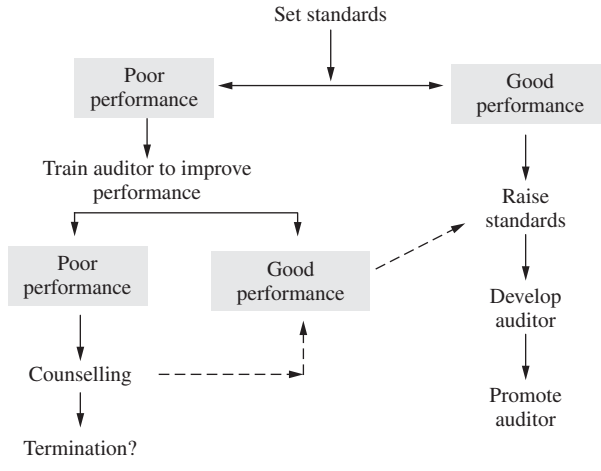


FIGURE 8.14 The auditor appraisal process.

'advancement', 'excellence', and 'quality' may each promote a positive environment. The counter-argument is that this positive environment has to be firmly in place before any performance appraisal can be planned. Whatever the view, it is essential that auditors are appraised in a positive fashion. This in turn depends on:

1. keeping the accent on praise;
2. not using the appraisal scheme to criticize but using it to develop;
3. using performance appraisal to engender good communications and listening skills;
4. seeking to promote a win/win environment where all sides gain.

Appraisal Criteria

There is no way that auditors can be appraised without reference to a formal appraisal criterion. This would be based on the types of skills, abilities and attributes required to discharge the audit role. The idea is to employ, teach, develop and improve each of these factors through a formal process of appraising each auditor's ability to achieve these standards. These performance standards may cover:

- basic auditing skills that all auditors should possess;
- advanced auditing skills that should attach to more senior auditors;
- managerial skills for auditors with staff responsibilities;
- skills in related specialist areas such as computing, accounting, facilitation, law and so on;
- other skills as required.

We are moving closer to defining a job specification that may be used to appoint audit staff. The same personal requirements may be applied to appraising the staff along with a series of personal targets. Higher levels of audit management need to acquire different types of skills as in Figure 8.15.

The performance appraisal scheme must cater for the above factors if it is to have any relevance to the internal audit function. Superimposed on this are special projects which may be developed by the auditor and one such typical basket of targets is shown in Table 8.1.

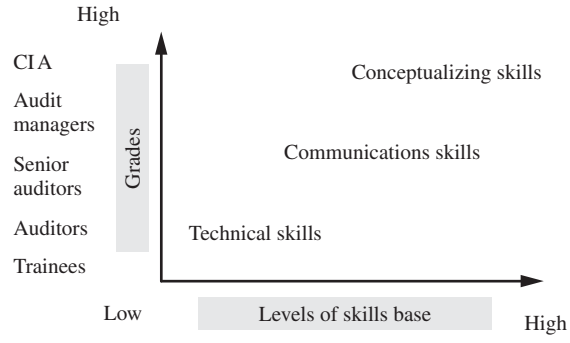


FIGURE 8.15 Different skills levels.

TABLE 8.1 Range of performance targets.

Source	*Targets (examples)*
Job description	Completing audits to budget and quality standards (audit manual)
Delegated tasks	Implement a new time monitoring system
Special projects	Restructuring exercise for the audit department
Personal development	Better communication skills, e.g. making oral presentations

Factors for Implementing an Auditor Appraisal Scheme

It is one thing to design an auditor performance-appraisal scheme but quite another to implement it in such a way that it produces the desired results. What looks good on paper may be different in practice. There are several matters to be considered including:

- The scheme must in fact address the auditor's performance. It should not be an alternative method of getting rid of problem staff or simply a paper exercise. The key objectives must be to assess and then seek to improve the performance of auditors at all levels in the internal audit department.
- The scheme should attempt to meet employees' needs, which should be based around a desire to obtain feedback on their achievements and approach to work. It can be sold to staff as a mechanism for providing this all-important feedback as opposed to just another management technique to increase the work rate.
- The scheme should represent a source of challenge to the auditor. The process of working to one's own personal targets engenders a form of maturity from staff but can lead to an assortment of soft targets being defined. Extremes can occur where parts of these personal targets may have already been achieved before they are applied. This positive approach can only be used in audit departments that employ highly motivated staff and use team-building approaches to work.
- The scheme must incorporate the concept of regular progress reporting. This is much better than an annual scheme whereby reports 'appear out of the blue' every 12 months. Ongoing assessment makes it easier to assimilate the scheme into everyday work that the auditor carries out.

- An auditor can compile a career plan as long as there is an awareness of the areas that have been developed and those that need further developing. A short-cut to this process is via the performance appraisal scheme that isolates one's strengths and weaknesses. To be valid the scheme must incorporate this feature rather than simply result in a finite category in the ranges of say 1–5. We have shown that auditors bring to their work a whole range of skills that together comprise a unique package. To simply classify a person as a category 1 (very poor) or 5 (very good), or a range between these two figures, is bad management practice. Unfortunately, there are many audit sections that do just this and still have difficulty working out why their particular scheme appears to demotivate their auditors.
- We can build on this idea of motivation by suggesting that any valid scheme should be geared directly into this concept of releasing 'people power.' Performance appraisal must as the bottom line exist to improve performance. As such it must then feed into a suitable development plan that gives a sense of direction and purpose to staff as they work for an organization over the years. This simple notion is sometimes forgotten when a scheme is introduced and fast becomes a weapon of terror in the wrong manager's hands. Note that what may be acceptable in a recession, when the supply of auditors exceeds demand, may be resented in times of high economic growth.
- The scheme should acknowledge the personal goals of each auditor. In this way, we should seek to establish a bridge between the organization's and the auditor's own targets. If the performance targets can become personal targets, then the appraisal scheme will run automatically as it is driven by the auditor's motivation, as opposed to an obscure set of goals.
- The appraisal scheme should ideally feed into a suitable training programme. This being the case, the scheme will hopefully be used to isolate any training needs that must be met to fill gaps in the skills required to perform at the appropriate level. There is little point in identifying skills gaps without seeking to close them. Such an approach whereby training is applied to problems makes the scheme more dynamic as a positive technique rather than concentrating merely on the perceived weaknesses.
- Performance appraisal should be sophisticated enough to define an auditor's potential to work at a defined level. This requires extrapolation to move the historical achievements into projected areas. The only imponderable is the impact of training and development plans. A learning rate may also be estimated so that one uses three key factors to arrive at the auditor's potential performance (Figure 8.16).
- Using the bridge between performance appraisal and auditor development plans, we can go on to consider the future of each auditor in terms of promoting his/her management skills,

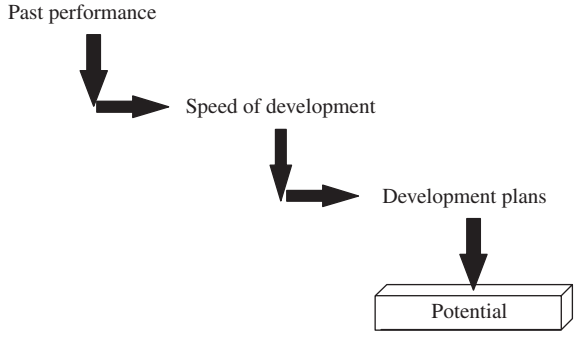


FIGURE 8.16 Auditor development rates.

existing job, and future potential. Again the idea is to get the scheme into a positive mode that is well received by staff.

- Counselling is also an important component of an appraisal scheme. Where the scheme isolates poor performance, this can lead to a great deal of stress for the auditor in question. One final implication of poor performance may be transfer/removal/dismissal. This is necessary as a final remedy that hopefully will never have to be applied as long as staff are willing to work and possess the basic skills that underpin this work. If we have to follow a line from the performance appraisal scheme to the poor performance procedures that may result in the removal of the auditor, there needs to be an interim stage based on counselling. This will seek to uncover barriers to performance that may be dealt with in addressing an inability to perform to required standards. Where these barriers can be eliminated, then the final transfer decision may be delayed and the auditor given what may be seen as a second chance. Here special support programmes should be in place to address this problem. Note that counselling should not be left entirely to audit management but must include a professional input from, say, the personnel department. The CAE should always remember that some employees perform badly because of their managers and this factor is often hidden from view as an interpretation of events is provided by the same manager. Again a level of sophistication built into the scheme is the keyword.
- We arrive at the final point of the principle underpinning performance appraisal which is the key ingredient: feedback. Performance appraisal provides an opportunity for the manager and audit staff to discuss performance as an issue and so develop the necessary mechanism for this feedback. Without stating the obvious, this feedback is a two-way affair. It requires both sides to listen to each other and develop a meaningful rapport along the following lines (Figure 8.17).

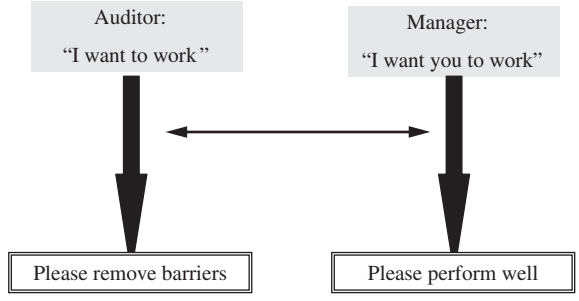


FIGURE 8.17 Feedback and appraisals.

Performance appraisal is less of a bureaucratic management technique. It is more of a vehicle through which performance can be addressed and developed by way of a close working relationship between the auditor and audit management.

Methods of Staff Appraisal

There are a variety of methods that are used to assess performance. Fortunately the internal audit arena, because of the nature of the work, provides a ready-made avenue through which auditors may be assessed. This is based on the audit review procedure where audit work is considered by audit management before it is signed off. Ways that auditors may have their performance assessed are:

1. The audit review process. Here we can use a standardized form to allow the manager to comment on the way the auditor carried out a piece of work that can then be copied onto

the person's personnel file. This brings appraisal naturally into the review process based on the hands-on work that the auditor performs rather than vague concepts.

2. A periodic review may be undertaken that deals with the auditor's performance, say, on a quarterly basis. Here one might simply take each item from the auditor's job specification along with special projects that have been assigned, and indicate the extent to which the required standards have been achieved. The manager must have reference to valid material to form the basis of this assessment and to this end one may refer to the jobs that have been charged on the auditor's time sheet.
3. It is possible to set performance targets for each auditor based on the annual/quarterly plans. This will be based on completing defined audits, keeping within budgets, performing special tasks such as the audit manual, and achieving a percentage of chargeable to non-chargeable hours. Where these targets flow from the overall organizational/departmental targets, a form of management by achievement ensues and hierarchies may be developed so that goals cascade downwards. Examples of some specific and team and overall unit performance targets may be listed:
   - extent to which the annual and quarterly plan has been achieved;
   - the percentage of recoverable hours charged;
   - time taken to respond to management requests for assistance;
   - staff turnover;
   - absenteeism rate;
   - number of improvements to the audit manual;
   - time taken by auditors to get access to audit management;
   - level of managerial agreement to audit risk criteria;
   - level of involvement of auditee in the audit terms of reference;
   - number of recommendations agreed upon;
   - level of complaints;
   - level of staff grievances against management;
   - time taken to issue audit reports after completion of the audit;
   - level of suggestions from staff to audit management;
   - level of compliance with the audit manual;
   - regularity of group and departmental meetings;
   - the percentage of staff with poor timekeeping;
   - number of aborted audits;
   - level of problems found during work reviews;
   - extent to which audit objectives have been met;
   - number of audits completed on time;
   - level of audits within time budget;
   - number of auditors passing professional exams;
   - number of audits delegated by the audit manager;
   - level of draft reports requiring rewrites;
   - extent to which developmental plans have been achieved;
   - extent of audit automation;
   - rate of production of audit products;
   - currency of time-monitoring information;
   - currency of time sheets submitted and authorized;
   - level of satisfaction from the clients;
   - extent to which desks are kept clear;
   - extent to which files hold all relevant information;

- time taken to find specific files;
- extent to which follow-up audits find that recommendations from previous reports have been implemented;
- number of audit reports issued;
- amount of alteration as a result of management review;
- level of recoverable hours to non-recoverable hours charged in the period;
- degree to which auditors keep within the budget hours for each audit;
- extent to which work plan has been completed;
- level of positive comments from clients via satisfaction questionnaire;
- level of absences from work.

There are drawbacks in defining auditors as belonging to a certain performance group or category. It is nonetheless possible to rate each range of the performance factors by assigning a figure. It is the final overall figure that creates the problems and as such this average or aggregate need not be calculated. The auditor's job specification has been quoted as one way of setting a suitable framework for the performance-appraisal scheme. Most argue that performance appraisal tends to highlight existing problems rather than cause them. The concept of appraisal must be set within a mechanism to codify what should be the best management practice in dealing with staff. There are many things that could go wrong with performance appraisal schemes when they are applied in an inappropriate fashion. It is important that there is a control over this process not in terms of an appeal, but in terms of referring matters for review. For this reason, it is possible to allow auditors to have specific concerns referred to the CAE to seek reconciliation or any amendments (if required). This review should revolve around the annual report and should be related only to matters connected with setting targets, reviewing performance and/or defining the resultant career development action plans. Professor Garry Marchant has highlighted typical complaints about measurement systems:

- Measurements are not in tune with strategic objectives.
- Measurement is conducted in isolation rather than systematically.
- Measurements are not customer driven.
- Financial measures are too late for any corrective action and encourage a short-term focus.
- Many key non-financial performance indicators are ignored.
- Measures are often used for punishment rather than for learning.
- Many measurement systems are rigid and non-adaptable.[10]

Good Appraisal Schemes

There are additional factors to consider when devising and implementing an appraisal scheme for the internal audit function:

1. They should be continuous and not periodical.
2. They should be accepted by the vast majority of auditors. Where this is not the case, the scheme will probably lower motivation levels rather than have a positive impact on the audit service.
3. The audit managers should also be subject to appraisal and this may be on the basis of the overall performance of their audit groups.
4. Training is required before any sensible scheme can be applied or the 'stick to the norm' tendency will arise.
5. Targets may cascade downwards to ensure that they are linked into organizational goals.

6. They should be linked into the underlying culture of the audit department and depend on whether a group basis is applied or one is seeking to promote individual working rather than teamwork.
7. Appraisal interviews should be carefully managed and used as a positive vehicle for open discussions in a confidential but structured format.
8. The scheme should result in at least a formal annual report that is held on file for future reference.
9. The underlying documentation to support the scheme should be devised and standardized as much as possible.
10. The scheme should be directed towards professional auditing standards.
11. They may be linked into financial rewards, although it is best to allow the scheme to operate for a while (at least a year) before it is amended to impact on the auditor's remuneration.
12. The CAE must be on guard for prejudice and must insist that audit managers bring to his/her attention any issues that may interfere with the smooth running of the scheme. Furthermore, the way the audit manager has operated the scheme should be reviewed by the CAE.
13. Each scheme should contain clear objectives that have been derived from a systematically applied procedure. In general, the more senior the job, the more demanding the targets.
14. One way of forcing managers to make clear decisions is to use alternative categories that one must select. This must, however, be accompanied by a suitable narrative that supports this choice. No overall mark should be assigned.
15. One should avoid using personality measures unless this is specifically asked for in the job specification. Even where this is the case, it is notoriously difficult to measure them if they are not linked into a specific skill.

Link into Career Development

The concept of appraising staff must attach to some form of professional foundation for it to have any real meaning. If it is not seen as part of a career development programme, then we return once more to the view that appraisals can have a demotivating effect on the auditor. Appraisals should be founded on a two-sided agreement that seeks to assess the auditor and then helps him/her address any identified deficiencies. Training, rotations, secondment, work assignments, staff assignment, skills workshops, special projects and so on are all valid techniques for developing staff based on their appraised needs. The key is to apply the right method, to the right auditor, for the right reasons.

Training and Development

There is a separate section on audit training that deals with this topic in some detail. Here we can simply state that there are different types of training that may be applied to meeting skills gaps identified through the performance appraisal scheme. Not only is it important to select the right training scheme to meet skills deficiencies but there should also be a formal method through which the results of such training can be assessed. Development, on the other hand, is a wider concept that entails many different activities. Development programmes are aimed at getting the auditor to maximize his/her potential within the internal audit function. Once performance targets have been set, there are many different ways in which an auditor may be developed to meet these targets including:

- rotation between audit groups;
- secondment to other departments/organizations;
- assignment to increasingly more difficult projects;
- assignment to specialist areas of audit work;
- additional managerial responsibility;
- special tasks such as the audit manual, audit planning, the IT strategy, risk appraisal, etc.;
- attendance at external groups such as an interorganizational IS audit working group;
- opportunities to deputize for a more senior auditor.

The idea is to develop and extend the skills database and so set the scene for career progression. In this way, the auditor's promotion is not derived from the performance appraisal scheme but he/she uses personal development to seek and obtain promotion. Training and development which is geared towards poorer performers is equally important, simply to get the auditor's skills up to a sufficiently high standard. In this way, no member of internal audit is left out of the equation that caters for all performance levels (as long as they meet basic minimum standards).

Client Feedback

There is a growing view that internal audit is primarily about providing a service to management. The more one is in tune with client needs, the better the final impact of the audit product. Client contact is the result of the many meetings and discussions between individual auditors and individual line managers, as well as the formal presentations by the CAE to the audit committee. The auditor's individual development programme should incorporate a consideration of client relationships, both in terms of appraising the adequacy of existing skills and with a view to developing them wherever possible. The section below on quality assurance outlines the use of client questionnaires that should follow the completion of each audit. The information contained therein should also flow into the auditor's development programme. The CAE should seek to develop the relevant communications skills in members of staff, for example:

1. An ability to appreciate the needs of auditees and seek to incorporate these into the audit work that is performed.
2. Good interpersonal skills and an ability to communicate in an open and friendly fashion. We could dedicate an entire book to this subject in view of the importance it holds for the success of the audit service. It is no exaggeration to suggest that this may be the single most important skill in any auditor, on the assumption that basic audit skills are in place. The excellent auditor will display these communication skills and a naturally acquired capacity to converse with all levels of client management.
3. An ability to work with managers in tackling risk and control deficiencies. We have discussed the participative approach to auditing early on in the handbook and this requires a basic ability where the auditor is able to bring this practice to life and work in a joint problem-solving mode.
4. Lastly, we should note that there must be a mechanism for receiving and dealing with complaints from clients that is independent of the auditor being complained about.

Counselling

Most of management's input into an auditor's career development programme will be quite positive, based on helping the auditor grow and progress. However, there will be times when

management has to address staffing issues arising from poor performance or behavioural problems and this will impact on the person's development. One model that may be applied breaks down staffing issues as shown in Figure 8.18.

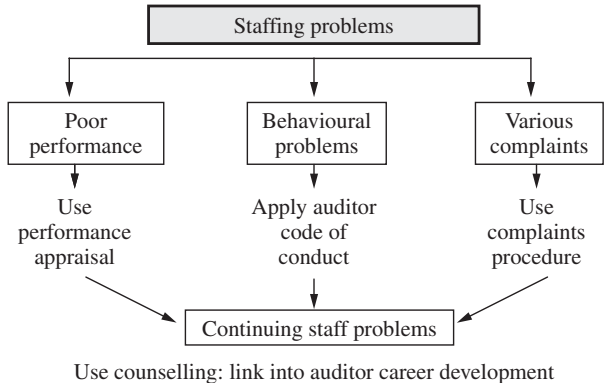


FIGURE 8.18 The application of staff counselling.

When applying counselling, audit management should take expert advice (from personnel) and ensure that they address the underlying problem and cause. It is an opportunity to discuss personal issues in confidence and understand how and why they are impacting on the auditor's performance at work.

Overall Productivity

Productivity is a fairly simple concept that suggests inputs produce outputs via a suitably controlled process. One measure of the effectiveness of this control is to set standards for the output based on the defined level of inputs. These standards become targets and so long as mechanisms for measuring the work have been installed, productivity can be assessed in terms of the extent to which these targets have been achieved. Career development uses performance measures as one way of measuring the way the auditor is developing and productivity factors are one feature of such a system. In this way, audit management may gauge an auditor's progress through quantifiable factors as well as more subjective considerations. We must always appreciate the limitations of productivity measures, which may appear scientific, but are based on underlying (and subjective) principles that have been agreed upon by management. The only real feature is that they may promote a degree of consistency across staff if they are applied in a systematic fashion. They may also provide a sense of direction for development plans by highlighting some of the targets towards which we are seeking to develop staff. The standard SMART test applied to target setting is based on the following model (subject to variations):

S: **S**pecific
M: **M**easurable
A: **A**chievable
R: **R**esults oriented
T: **T**ime based

For example, a target for a senior auditor may be:

> To prepare and implement a new and revised audit manual that complies with best practice and adopted audit standards by date X (using 100 audit hours).

Attached to this would be various performance measures that could form the basis of reviewing the extent to which the targets have been achieved. These measures could include:

1. **Time budget** – one-third of work should be done by 33 hours, one-half by 50 hours, etc.
2. **Time frame** – the due date should be kept under review.
3. **Qualitative** – all key areas in line with professional audit standards should be covered.
4. **Acceptable** – the draft manual should be accepted by audit management.
5. **Implemented** – plan to get the document implemented should be drawn up and achieved.

Single Audit Evaluation

One key factor in any development programme must be the ability to perform an audit. This may be seen as the basis of success in that, if each audit is performed well, we have a good chance of delivering a quality audit service. The management review process that is applied to an audit before it is signed off provides an opportunity to assess the auditor's performance and so build this into the various career development programmes. As such the review process should incorporate a judgement as to the adequacy of the application of auditing procedures by using the following approach:

1. Audit manager reviews each aspect of the audit, both as it progresses and after it has been done. Compliance with the standards established through the audit manual would feature in this review as will the overall 'feel' of the audit.
2. Any deficiencies should be highlighted for action and correction by the auditor in question.
3. Relevant points arising from the above should be assimilated into individual auditor's development programmes where there are obvious problems dealing with some aspects of the audit.
4. A suitable document should be extracted from the audit file for inclusion into the personal performance appraisal file for the auditor/s in question, based on the review points. This will address the question: How did the auditor perform in this piece of work?
5. They should then be linked to the audit post specification in terms of defined audit skills and attributes that should be seen in action during the audit.
6. Action should be taken to address any auditor weaknesses. Remember to look out for any special accomplishments as well as problems.

Leavers

Career development programmes give direction to staff and help them achieve a sense of purpose in their work and their plans for the future. It tends to create a positive culture where auditors, in the main, wish to stay with the organization and do not necessarily have to leave to achieve their career goals. This is not to say that staff should not leave and pursue career adventures outside their current employment. We should, however, be concerned about auditors who leave because they are unhappy about their development in the internal audit department. As such,

audit management should establish a mechanism whereby it may identify any problems with development plans that have led to staff resignations. Exit interviews are one way that this may be carried out as long as the right questions are asked and management acts on any information obtained from this source.

In terms of the overall performance measures for the internal auditing department, the IIA.UK&Ireland have carried out a survey of almost 200 audit functions on some key benchmarking measures, in order of importance:

	companies using the PI %
Customer satisfaction questionnaires	39
Completion of audit plan	37
Utilization rates	31
Turnaround time of fieldwork to report	31
Audit costs compared to budget	27
Recommendations accepted by auditee	25
Implementation of recommendations	15
Quality of recommendations/report	16
Business impact	9
Number of audits performed	8[11]

There is no reason why internal audit should not take advantage of the balanced scorecard in establishing performance measures. The Society of Management Accountants of Canada has prepared a resource that explains the four categories of the Kaplan and Norton model:

1. **Financial.** The first category on the Kaplan and Norton balanced scorecard is financial. Managers devising financial measures should ask themselves, How can we show our strategy is succeeding financially? At the highest level, long-term profitability and stock price growth demonstrate financial success of the strategy. But managers should also consider financial measures particular to their strategy. If the firm is young, on a high-growth trajectory, sales growth by sales channel may be a critical financial measure. If the firm operates in a mature business, cash flow may be the right measure. If it falls in between, economic profit, a measure that charges the company for the cost of equity capital, may be the right measure.
2. **Customer.** The second box in the Kaplan and Norton model is the customer perspective. Managers devising customer measures should ask themselves, How can we show we're delivering to customers the value they expect? At the highest level, many companies track customer satisfaction. But other measures are also necessary, like customer retention, market share, and share of wallet (i.e., share of a customer's business in a particular product or service line). Companies may also devise specific surveys. For example, Eastman Chemical surveys companies to find out how they score Eastman on 'customer value.'
3. **Internal business process.** The third box in the Kaplan and Norton model is internal business. Managers developing measures for this perspective should ask, What processes must we excel at to deliver value to our customers? For example, Analog Devices measures chip yield, cycle time, on-time delivery, and parts per million defects to gauge the performance of manufacturing processes. CIGNA Property & Casualty, the Philadelphia insurer acquired by Ace Ltd. of Bermuda, developed a system to measure underwriting quality (by survey) and loss ratio (claims paid divided by premium collected) to gauge the quality of its underwriting processes.
4. **Learning and growth.** The fourth box in the Kaplan and Norton model is learning and growth. For this perspective, managers should ask, What action must the company

take to prepare the people and organization for the future? As an example, CIGNA Property & Casualty developed measures for competency development, key staff turnover, and acquisition of key staff. Whirlpool developed measures of variables such as completion of cultural milestones and, by survey, strength of leadership, commitment, and diversity. The measures in the learning and growth perspective stress reskilling, systems development, change procedures, and development of personal and organizational capabilities.[12]

Enhancing Your Internal Audit Performance

By Dan Swanson, *Compliance Week Columnist*

The internal audit function's position within a company is unique. It provides its principal stakeholders (audit committee members and management) valuable and objective assurance on governance, risk management, and control processes, as well as consulting services to improve operations. With this critical responsibility to fulfil, implicit in executing those duties is internal audit's continuous improvements to its own practices. How do you do that? A high-quality internal audit function meets or exceeds stakeholder expectations, while ensuring that value is added to the organization. The most critical factor in achieving internal audit quality is the auditor's competency and proficiency in evaluating the organization's risk-management, control, and governance processes. Each internal audit department should have a program not only to ensure top quality of internal audit reports, investigations, consulting, and other services, but it should also have a way to effect continuous improvement in its service to stakeholders.

Steps to Success

The Institute of Internal Auditors recently issued a ''quality maturity model'' that includes a roadmap for improving internal audit practices over time. The model comprises five basic levels:

Level 1: Introductory. The internal audit function at this level has no quality assurance and improvement program in place. Typically, a Level 1 internal audit department would be fairly new or one that has not yet conformed to the quality requirements within the IIA's International Standards for the Professional Practice of Internal Audit. In other cases, the chief auditing executive or the audit committee lacks a clear understanding of the substantial value that such a program can bring to an organization.

Level 2: Emerging. The internal audit function conducts periodic and ongoing self-assessments, or internal quality assessments, monitoring the department's compliance with the Standards.

Level 3: Established. The internal audit activity obtains an independent evaluation of its self-assessment and improvement efforts at least every five years.

Level 4: Progressive. A quality assurance and improvement program is integrated into the operations of the internal audit activity. The activity generally complies with the Standards and Code of Ethics, and obtains an external quality assurance review at least every five years.

Level 5: Advanced. An active and fully integrated quality assurance and improvement program exists within the daily operations of the internal audit function. An external QA is conducted at least every three years. All staff members follow a rigorous continuing education program.

In most enterprises, the audit committee oversees the internal audit function. As such, audit committee members should have direct interaction with the leadership and activities of the internal audit team and should monitor the internal audit team's performance. Using the quality maturity model's guidance to discuss regularly the internal audit department's continuous improvement efforts will encourage a world-class audit function. Regular revisiting of internal audit department's quality ''progress'' will also influence the motivation and focus of the audit team.

Other Board Guidance

The IIA's briefing paper, Internal Audit Standards: Why They Matter, presents a series of questions to facilitate a closer relationship between the audit committee and internal auditing. This guidance also provides a summary of typical audit committee oversight responsibilities. Directors of enterprises that have internal audit departments are expected to determine that the IA function works effectively. Where an internal audit function has not been formally established, these questions should be discussed with senior.

The IIA has also issued the landmark board-level guidance, 20 Questions Directors Should Ask About Internal Audit, to help audit committees develop a better understanding of, and establish performance standards for, the chief auditing executive's activities.

The first important area to explore is the mandate of the internal audit function, including what services it should provide and what its priorities should be. Ask yourself: Is internal audit focused on the right things? For example, does the IA function evaluate the company's efforts to establish an effective enterprise-wide risk-management program? Another important topic is the audit committee's relationship with the internal audit function. Here, the key issues are whether the internal audit activities are supported by the audit committee (for example, ensuring appropriate prominence on the organizational chart) and what influence management has on the internal audit function through its organizational structure. Are there open lines of communication between the chair of the audit committee and the chief audit executive? Is there an executive session with the CAE at every audit committee meeting to ensure frank discussion?

A third concern is resources. Does internal audit have the appropriate level of resources with the right skill sets to produce world-class results? If not, auditing of the business and the depth of analysis can be inappropriate. Internal audit requires highly skilled resources, and the competition for staff becomes more difficult each year. A long-term workforce plan would be very beneficial in today's complex and fast-changing business environment. An annual audit committee review of internal audit and enterprise-wide human resource planning can be invaluable.

Finally, the results of the internal audit efforts should be reviewed regularly by the audit committee, and an overall determination made about whether the audit

committee is satisfied with the information and performance it receives from internal auditing

Adopting Excellence

Confirming that your internal audit function is on the road to quality – and consequently helping to ensure the ongoing value of your internal audit activity – will bring great benefits to your organization and its stakeholders. A few steps CAEs should consider taking:

(1) Educate themselves and their staff in quality practices.
(2) Define their stakeholders; shareholders, the audit committee, executives, corporate management, and business unit managers, at the least; perhaps more for your specific enterprise.
(3) Brainstorm with staff. Let them tell you what they see as their collective strengths and weaknesses. What do they need and what do they desire to become more effective and productive?
(4) Involve stakeholders in an initial conversation about expectations and needs; conduct brainstorming sessions and determine what you do well and what areas need improvement.
(5) Create, distribute, and tabulate a survey for your various levels, and implement change improvements.
(6) Periodically review your progress, and determine where additional change and improvement is needed.
(7) Continue to track those areas where you can be most effective. Publish your accomplishments and improvements.
(8) Engage outside fraud investigators to teach internal auditors what to look for, and have them work with auditors on internal cases to help auditors appreciate what they are looking for and how insiders try to hide those things. Consider the use of other outside specialists as department needs dictate.

The audit committee, meanwhile, has some questions of its own that it should be asking:

- Has a quality assurance and improvement program within internal audit been established? What are the results to date?
- How do we know the internal audit function is effective? What are the key performance measures and results to date? How many frauds have been detected through audits per year? Are the rates of detection changing from year to year, and why or why not?
- What kind of control weaknesses, revenue gains, or expense reductions have been identified? Is internal audit making an impact?
- How is the internal audit function doing in relation to the International Standards for the Practice of Internal Auditing? What are the strengths and weaknesses of the internal audit department?

Is your organization's internal audit function practicing what it preaches? That is, has internal audit established a long-term continuous improvement program? Finally,

is the audit committee doing all it can to ensure the internal audit function has the organizational status, independence, and objectivity to complete its mandate effectively?

The bottom line is that improving the internal audit department's performance will help improve the whole enterprise's performance as well. That is, effective internal auditing can be leveraged across the company. The audit committee must provide effective oversight over internal audit. By using the right guidance and by asking the right questions, it can do just that.

Reprinted from *Compliance Week*. This article was originally published in Compliance Week. Reproduced by permission of Compliance Week. All rights reserved.

8.4 Dealing with Typical Problems

Perfection is impossible to achieve although inefficiency should be contained within acceptable levels and controlled. Audit management is responsible for developing strategies for resolving problems in internal audit. Turning a blind eye to poor practices and not demanding relevant control information are practices that impair good service delivery. If audit managers do not ask for reports on budget overruns on audit jobs, they are guilty of mismanagement/maladministration. If time sheets are not being filled in accurately to reflect time spent, then management must react. The worst case is ignoring internal problems while at the same time auditors are seeking to promote high standards of control from audit clients.

> During an audit, a senior auditor wished to advise management to sort out the filing system which was untidy, with files left out over desks, cupboards and the floor. Unfortunately this was not possible since the audit manager's own office was the most untidy and disorganized in the entire organization.

Excess Hours Charged

This can be a problem area. Audit resources can be regarded as the sum of chargeable hours. Time is the most important factor that must be controlled by audit management which requires:

1. authorized budgets set for jobs;
2. time sheets accurately recording hours spent on the job;
3. regular reports on hours charged;
4. effective management action.

If there are weaknesses in any of the above, then this control will not operate properly. Even where this system is in place, there may still be excess hours charged to jobs. This occurs where:

- the budget was not set properly;
- the budget is not seen as a serious issue;
- authorization was not secured for extended hours;
- the audit entailed resolving unforeseen problems and/or difficulties;
- the client asked for additional work;

- the auditor decided to do additional work;
- the auditor was 'dumping' time into the job; not all charged hours were worked on the project;
- the auditor was inefficient;
- the audit manager caused extra hours to be charged by excessive intervention or lack of it.

Effective management action requires communication, involvement and consideration if this system is to work and play a positive role in controlling audit projects.

Inadequate Working Papers

There are often inadequacies in working papers although this may be trivialized as a minor issue that detracts from the important issues that concern audit management.

> A new audit manager was given a draft report to review. She asked the field auditor to provide the working papers. The auditor could not find them at first and after some time extracted a file of loose documents from under his desk.

Findings from internal audit reports and files play an important role. It is insulting to produce a report for management that has no clear supporting documentation prepared to defined standards. Even where the report is accepted by management, we should be able to confirm all important material that has been reported. Priorities need to be addressed. Audit management must as a minimum:

- set a documentation standard that covers permanent and current audit files;
- train staff in these standards;
- review all audits and seek compliance with the standards;
- review the filing system: destroy old files or microfilm, archive or retain them on disk;
- maintain a 'clear-desk' policy that ensures files and papers are not scattered;
- adopt automated papers;
- use standardized documentation;
- keep the documentation standard under review.

No Sense of Direction

Auditors carry out required work and issue assurances and advice to management. They assist management and are seen as experts on corporate governance, risk management and internal controls. Reports give recommendations which may or may not be acted upon by management while, as time goes on, these reports fall out of date and new work is required that takes current circumstances on board. We may be auditing a moving target where operational areas undergo continuous change, many of which are confidential and the auditor may make recommendations when not sure what major changes are planned for the immediate future.

> An auditor was coming towards the end of a major review of the payroll section (based in the finance department) that covered the way staff were organized and directed to achieve

control over this function. Management had prepared confidential papers to decentralize payroll with only a core service at the centre. On receipt of the draft audit report, management was impressed but felt it would be superseded by their major changes.

It would have been better to setup internal audit up as consultants to assist the confidential change project. There is great danger where the audit role loses direction and operates on autopilot churning out report after report with little meaning to the organization or the auditors themselves.

A new audit manager with many auditing qualifications was eager to use his newly found knowledge to embark on management audits. He briefed a senior auditor, who had been in internal audit for many years, about a new audit assignment. The auditor showed little interest and eventually commented that 'I will be OK as I remember doing this audit five years ago.'

A loss of direction can be the difference between a good audit and a boring report. Demotivated auditors are a problem for audit management even where they do their work and keep within budget. They will not contribute to the development of the audit function or inspire others to produce excellent work. Admittedly some auditors cannot be motivated. The CAE should:

1. prepare and implement an audit strategy that pushes internal audit from one period to another;
2. publicize this strategy and seek support from staff by involving them in its formation and use;
3. market internal audit and recognize achievement so that staff can relate to success criteria;
4. implement suitable HRM policies and programmes;
5. remove blockages to performance, particularly with awkward clients who may impair audit's right of unrestricted access to documents, records and information;
6. keep internal audit fresh and vibrant by regular section meetings, days out, seminars, social events and an invigorating audit manual;
7. have clear goals.

No Follow-up Procedure

Another weakness is lack of follow-up procedures. Auditors adopt the attitude that they do the audit and simply walk away. The follow-up procedure is less of a formality and more an acceptance of responsibility for the audit. The internal auditor needs to:

1. target high risk systems;
2. review the adequacy and effectiveness of the systems of control that protect this system;
3. alert management to any problems with these controls where necessary;
4. advise management of ways that systems of control may be improved to handle risk;
5. ensure management responds to audit findings and indicates what it intends to do;
6. monitor the action taken by management;
7. revisit the audit after a suitable period to highlight further action management needs to take in respect of its controls.

Much of the above results in recommendations being made to managers on the action they need to take in tackling risk and improving controls or investigating related matters. Many recommendations talk of the need for urgency in addressing outstanding concerns identified during the audit. To leave the audit after publication of the report and show no concern to follow-up issues that were left with management sends out the wrong signals. The follow-up routine is a key ingredient for any audit and it motivates staff by providing an end-product where required changes are properly actioned by management.

Low Pay

This is a problem in some internal audit departments that has a causal effect by impairing the ability to deliver good audit services. The knock-on effect of low pay is:

- low status;
- inability to attract good calibre staff;
- inability to retain good calibre staff;
- less scope to implement development strategies within the function;
- inability to deliver an adequate audit service.

Inadequate Audit Manual

An indicator of the adequacy of an internal audit function is the condition of the audit manual. If it is out of date, unused or inadequate, audit management has failed to provide clear standards, policies and procedures for the performance of audit work. The manual is not a low priority item considered only when there is spare time available. One argument is that smaller units who employ senior auditors may not need to adopt the rigours of a formal manual. The clear requirement is that standards must still be set and applied even where staff are experienced. There is no escaping this, although the depth and scope of coverage of the manual may vary depending on the type of audit unit.

Poor Planning

There are internal audit departments that work to no formal plans. They provide a response-based service which suggests that what is important to management on any particular day should also be important to internal audit. Audit work consists of a constant stream of referrals from senior management who ask for a variety of matters to be investigated by internal audit. Audit responds, carries out the work, and all parties are happy. Planned audit work is not completed because all audit resources are diverted to consulting work. This imbalance is based on a failure to appreciate two basic concepts:

1. Internal audit works for the organization, and not just individual managers. The corporate organization needs its risk management and controls reviewed and made right while individual managers want help in dealing with specific issues that affect them day by day. Resources must be balanced to achieve both objectives.
2. Most management referrals consist of problems that result from poor systems and they call on audit to help them assess risk and review their controls.

Another imbalance is where inflexible planning means that planned audits consume too much of the audit resource and are focused around last year's issues. Good planning consists of a formal evaluation of the relative risks in defined audit units to direct audit resources towards those changing key risks that impact on organizational success with room for management requests. The audit plan represents a contract between the organization and internal audit. It sets out what should be done and when, while leaving enough space for consulting projects. There is also a need to develop an effective business plan. This sets the internal audit function up as a business unit with clients, marketing strategies and concrete business goals. Planning has come a long way and a commentary from Howard Johnson of JC Penny described this development:

> The days of copiously planning next year's audits several months before the start of the year are long gone in our audit department. To stay on top of the dynamic business environment, we employ a just-in-time approach to setting our audit plans. Instead of performing an autopsy of the past, most of internal auditing's work should be geared toward looking at the present and the future. And if we're going to be reviewing business priorities that affect current and future operations, then we must be flexible in scheduling our time. At JC Penny, we leave considerable time open in our audit schedule so that customers can make special requests for our assistance.

The planning timetable needs to be both fixed and flexible to take new developments on board. One planning system in use follows the pattern below:

- November – start the new planning process and build in extra capacity for consulting requests for management (via a formal assessment criteria).
- December – draft risk assessment forms and review of corporate risk database. One audit team uses the following allocations of productive audit time that is assigned in outline to: 50% annual audit plan, 20% emerging risk issues, 7% special investigations, 20% special projects, 3% follow-up.
- January/February – analyse information and talk to senior management and the board and include all agreed consulting projects in the audit plan.
- March – finalize the annual audit plan after discussing the draft plan with the audit committee.
- End March – publish the plan and allow update facilities.
- April – the plan is ready to be implemented.

Inadequate Supervision

The level of supervision depends on the type of work and auditors employed. For more senior staff this may be based mainly around the final review procedure, with little involvement from audit management during field work. For less senior staff, a lead auditor may be appointed or the audit manager may spend time with auditors on site. The amount of supervision should correspond with the need to exercise close control over the project. The problem arises where management has failed to provide the requisite level of supervision. This failing is related to a lack of procedures on how audits are controlled and supervised rather than the behaviour of individual audit managers. Auditing standards require the auditors to undertake only audits that they are able to perform. Auditors should not simply be left alone to carry out audits with little or no support from audit management. It is incumbent on audit management to assess the level of supervision an auditor requires. This dictates the extent to which direction and assistance is provided during an audit. There is a need to ensure that audit management/seniors are available at short notice, and this should not impact on any performance appraisal scheme. Seeking advice

should not be seen as an admission of failure. Only by setting suitable standards and ensuring that they are met can audit management discharge this role.

Lack of Continuing Professional Education

Another mistake is to forget that staff development is a continuing process and does not end with professional training. It is one thing to establish formal training programmes and support auditors in professional training, but we must not forget to view post-qualification training as another fundamental requirement. There are auditors who may not succeed in formal examinations and their training requirements cannot be ignored. The world of internal audit is ever-changing and what was taught years ago has to be updated to keep up with developments.

No Career Development

Successful internal audit depends on high levels of auditor motivation which is a key factor in career development. Where auditors believe they have no chance to develop and achieve higher grades and increasing levels of experience, they become demotivated. Audit can be a long-term career as long as there is development and ways to ensure that staff do not stagnate. Good staff will always be in demand but if reasonable expectations are not met, they will leave. Less-able staff will remain and reduce overall efficiency. Management must develop staff to reach full potential and develop into all-round auditors. Career development does not just revolve around increased financial reward. It is a factor, but exposure to the variety of audit work keeps staff interested without necessarily promoting them.

Reporting Delays

Auditors work well in the field through the psychological desire to perform well to an audience. They must be seen to be efficient. Some auditors pride themselves on receiving commendations from clients as they put in long hours. Unfortunately, this falls away when the auditor returns to the desk in the internal audit unit. Away from the client and among friends and colleagues, the temptation is to engage in office banter and open-ended conversations. Even with a work flavour, it takes time away from the main project. Where the department applies a policy of drafting audit reports back at the audit office this may lead to delay. The implications of excessive delays in reporting are:

- The continuity of the audit may be lost as the auditor works increasingly from files and relies less on hands-on images obtained at the audit site.
- The audit is de-prioritized by the client who sees the delay as an indication of low importance.
- Changes that are not anticipated by the auditor occur. This impacts on implementing the auditor's recommendations as they are superseded by new circumstances.
- The auditor becomes bored with the project impairing the quality of the final report.
- There is more chance of interruptions from urgent work required in other areas.
- The client may feel that the audit is aborted and not expect to receive a report.

Audit management must avoid this and the reporting stage holding up the audit process:

1. Introduce technology to ensure that reports can be prepared, copied and quickly bound in-house.

2. Set clear reporting standards so that structure and style are not reinvented for every draft.
3. Adopt standardized working papers to feed smoothly into the reporting system. Link papers to show terms of reference, findings, implications, conclusions, recommendations, client comment and agreed-upon action in a logical order that fits the report structure.
4. Write most of the report at the client premises as the audit progresses using laptops.
5. Set separate budgets for the reporting stage that are carefully monitored and controlled.
6. Set a reporting date standard of, say, three days after completion of the field work.
7. Ensure that the audit review process is ongoing and does not hold up progress of the draft report.
8. Ensure that auditors receive training in efficient report writing and drafting.

Lack of Professionalism

This amounts to a lack of qualified staff working to professional standards. Auditors with no formal qualification can perform to high standards. Professional and formal training programmes do, however, bring an injection of new research and ideas. There needs to be a foundation upon which the CAE may build an audit function and this comes from employing and developing professional staff. There is always room for people who do not hold qualifications although there must be a nucleus of staff who have passed formal examinations. This balance should deliver good services.

Financial Emphasis

There still exists the old-fashioned view that internal audit is primarily a branch of accountancy. The modern-day equivalent is the internal audit function whose role revolves around financial systems. Accountants discharge these responsibilities and will support external audit work. This traditional model of internal audit is easy to manage and may be in line with managers' expectations, but it has drawbacks. First, the potential of audit functions that can work on projects outside the financial arena will be missed. Second, the scope for overall development of audit skills and perspectives is restricted by this fixation with financial systems. Despite this, there are still internal audit units that hold onto the financial bias, and as long as it meets organizational expectations, it is hard to criticize them. It is up to the organization to realize the potential that can be derived from a top-level, unrestricted audit function and a dynamic CAE has a pivotal role to promote this vision.

Performing Line Functions

We have moved on from internal audit rubber stamping parts of the system and being part of line operations. The problems are more subtle now where, although removed from line roles, internal audit is still locked into the system. This occurs where managers refer their problems to the auditors for resolution. It may be a list of system errors, a breach of procedure or waste occurrence. Taking responsibility away from management and locating this with internal audit gives the auditor operational responsibility. Where we accept this situation for short-term convenience (and possibly compliments) there will be longer-term problems and poor appreciation of the duties and obligations of management. Where internal audit provides this fallback, it is as much a part of the system as it was in the days when it stamped each payment before the cheque could be released. A more appropriate response is for internal audit to advise management on how best to solve its problems and improve the way it manages risk.

No Defined Approach

The final problem is where internal audit has no consensus as to its approach to audit work. When describing an audit we may use a variety of terms including investigation, study, inquiry, examination, review, programme and project. Each carries a different emphasis and means different things to different people. There are different models of internal audit and the type of work that discharges the audit role. Short compliance-based audits last a few days while major operational reviews with wide terms of reference take several months. If this agrees with the audit charter and meets professional auditing standards, there is no reason why these differences should not exist. The problem lies when the CAE has not decided the right approach. Members of the audit department will be left to guess or make up their approach from personal experience. There is little scope to develop a professional audit service and associated procedures. There will be role conflict among audit staff if the approach has not been clarified, particularly between assurance work and carrying out consulting projects on behalf of management.

Link into Problems of Internal Audit

Each problem real or potential must be isolated and resolved if not to threaten internal audit. There is something wrong with a unit seeking to identify control weaknesses across the organization when the same unit has many predicaments that it is not able to rectify. If performance appraisal is seen as a key control over staff it may be recommended by internal audit. If internal audit has not been able to implement an appraisal scheme there is a dilemma. Another example is the conflict where internal audit recommends efficient information systems in operational areas when the audit office is piled high with old files, boxes of documents and an assortment of material, loosely related to old audit work. In one internal audit office, an old broken-down typewriter was confiscated for forensic testing that was not in the event available, and was left in a corridor in the audit offices for over five years before it was finally disposed of. The CAE must evolve a strategy that confronts foreseeable problems as a priority. The role of audit management need not be purely managerial. An alternative model is where audit management ignores their staff in favour of various special projects that they personally perform as top secret assignments. This type of manager will have little use in developing audit strategies. Only a small number of the potential threats that face internal audit have been referred to. There are a number of matters that impact on the ability to combat these threats:

- The CAE must ensure that threats to the future welfare of audit are isolated and dealt with.
- Scan the horizon, assimilate external influences and translate them into resources.
- The resulting research must be incorporated into a formal audit strategy that drives the function through a defined period, generally, of years.
- Possible threats may be subtle and may not necessarily affect internal audit directly, but may impair the ability to deliver an independent audit service to professional standards.

Dealing with Problem Staff

Clearly, the CAE has to establish sound codes of conduct and performance measures based on professional auditing standards. These are targets that are constantly sought after in terms of the

entire audit service and each individual auditor. Effort is directed towards moving the internal audit function closer to these targets as all levels of auditor contribute to this process. This is the upside of development where the push from all staff is in the same direction. The downside occurs where there are cracks in this model that, if left unattended, will impair the efficiency of the audit service. These cracks may result from problems created by the most unreliable of resources, people. Staffing problems must be resolved as quickly as possible and the best way to isolate them is by contrasting this behaviour with defined standards that are demanded from all staff. Hopefully, most staffing problems can be perceived as breaches of procedure and dealt with by management as such. There are unfortunately many problems that are caused by managers, particularly where they fail to deal with an issue in a timely way. Standards nonetheless are important. As an example, there is little action management can take against any employee who takes excessive sick leave, if the organization has not bothered to define exactly what is considered to be excessive.

8.5 The Audit Manual

The topic of audit manuals touches upon a number of subsidiary issues including standardization, procedures, controlling creativity and audit approaches and underpins professional standards for delivering the adopted audit strategy. *Brink's Modern Internal Auditing* has described the role of the audit manual: 'Audits need to be managed, and the best tool for audit management is an audit manual. An internal audit manual is an in-house guide to the contents of an audit; it is a reference book which can be consulted when an audit question arises.'[13]

This section brings together the main topics that should be dealt with via the audit manual, as well as discussing some models that help illustrate this all-important technique.

The Role of the Audit Manual

It is necessary to establish the role and objectives of the audit manual before considering appropriate models. Publications on internal audit procedures and performance bear on the topic and so a wide range of material has been considered. The IIA standard 2040 covers policies and procedures:

> The chief audit executive must establish policies and procedures to guide the internal audit activity.

The interpretation goes on to say:

> The form and content of policies and procedures are dependent upon the size and structure of the internal audit activity and the complexity of its work.

Our definition of the audit manual is:

> A device that involves the accumulation and dissemination of all those documents, guidance, direction and instructions issued by audit management that affect the way the audit service is delivered.

The manual is a mechanism for channelling guidance for the auditor. The available material provides comments from many different sources and will give insight into the various issues that surround the design and implementation of audit manuals.

Manuals fulfil the following roles:

Defining standards and methods of work This is the first and foremost task of the audit manual as the vehicle for defining auditing standards. The way audit will be managed and audit resources employed are matters that have to be decided by audit management in seeking to discharge its responsibility for delivering a quality audit service.

Communicating this to auditors The second role of the manual is to bring the requisite standards to the attention of audit staff. By including relevant material in the manual we can argue that this means they have to be adhered to by all staff by virtue of their position. Assorted memos, advice and documents issued to auditors have no real status if they are not delivered in a coordinated manner and it is here that the audit manual is of great assistance.

Establishing a base from which to measure the expected standards of performance As long as management has set standards and communicated these to staff (along with training if required) the auditors can then be expected to apply the standard. We then use this to determine whether audit staff are able to perform. Herein lies the third role of the manual in enabling management to consider and judge the performance of its staff.

In using this model, we return to the concept of the manual as a framework for processes that lift the quality of audit work. The question that then arises is: What mechanisms are used to establish an acceptable audit service in audit departments that have inadequate audit manuals? Although the main objectives of the manual may be clearly defined, the degree to which audit requirements are specified will vary, and the adopted manual may be more or less prescriptive depending on a number of factors. One might view the actual task of the manual as falling on the following continuum:

- to provide a range of reference material for auditors;
- to provide a general framework for the audit function;
- to provide a comprehensive guide to audit work.

These three definitions move from a basic through to a more comprehensive view of the manual with increasing degrees of guidance provided. The precise function of the audit manual will vary. A conscious decision must be made by audit management regarding which model to select based on the circumstances and an understanding of available models.

We can draw from this three section model by separating the managerial aspects from basic administration and adjust it to appear as shown in Table 8.2.

TABLE 8.2 Sections of an audit manual.

Section	*Contents*
Managerial	Concerning the management of the audit function
Operational	Concerning the performance of audit work
Administrative	All other procedural matters

It is not possible to be more precise than this. The great diversity in style and format of audit manuals is a natural result of the diversity in audit work, approaches and quality assurance mechanisms that are applied by chief internal auditors. What we can say is that in addition to the managerial, operational, and administrative headings, first, the objectives of the manual must be clearly defined and, second, the resultant document must be sufficient to achieve these objectives.

Standardized Forms

One issue is the concept of standardized documentation and the associated role of the audit manual. Before we touch on the topic of standard forms it should be clearly established that our definition of audit manuals is as a managerial vehicle for directing auditors. This means that standardized procedures form part of the formal standards that have to be achieved. To have documentation standards as ad hoc forms without coordinating them as a manual will necessarily cause inconsistency and inefficiencies in their application. There is an abundance of material on the advantages of standardization and a number of features can be highlighted:

1. The most familiar standardized procedures are in the form of internal control questionnaires and audit programmes that are developed by many audit departments. The general view is that what in effect are checklists must be tailored by the auditor or the audit objective can become immersed in the sole task of completing these documents. In many cases, this can lead to low-level audit work carried out by junior or inexperienced staff and a corresponding poor image for internal audit.
2. Flowcharts should follow a uniform pattern that should be consistently applied throughout the audit department. This enables one to direct training at a particular model that is in use and also ensures that different auditors are able to understand flowcharts prepared by their colleagues. This also applies to block diagrams and other simplified graphical models.
3. Standardization leads to consistency and report writing can have a 'house style'. We would expect audit functions to publish reports in line with an adopted standard that is well known throughout the organization. Audit reports may end up anywhere within (or outside) the organization and it is right that they follow a prescribed format.
4. Standardization can lead to auditors giving less attention to format and procedures and more attention to the actual objectives of the task at hand. We need not reinvent the wheel each time an audit is performed since standards once applied are used whenever the set criterion applies. Auditors should be more concerned with the underlying messages that are provided via the audit process and not the documentation and procedures applied to arriving at this position. The argument runs that audit management can give detailed consideration to a standard that can then be used by auditors as an efficient vehicle for performing their work.
5. Standardization can constitute a vital control over each audit assignment. The act of setting a standard also provides guidance over the relevant parts of the audit and this helps to give it form and direction. For example, we may state that all interview records will include a summary that indicates what impact the information has on the audit at hand. In this way, we will have forced the auditor to make this consideration which in turn will give better direction to the interview. This acts as a control over the interview process that stops them from drifting aimlessly if the audit objectives are not held in mind.

The position we have reached in defining a model audit manual is that all moves to standardize procedures should be channelled through the audit manual. This might be the biggest single

benefit from resourcing the implementation of a comprehensive and up-to-date manual. Lastly, the task of progressing an audit automation strategy depends largely on having standardized procedures that might be automated and a formal vehicle for implementing these procedures, i.e. an audit manual.

Procedures and Working Papers

The audit manual is the device that allows audit management to consider, formulate and apply suitable audit procedures aimed at ensuring efficiency as well as compliance with standards. It is difficult to visualize any other way that this could be achieved. It must be remembered that audit procedures cannot simply be extracted from audit textbooks but have to be adapted to suit the particular audit approach. The IIA Practice Advisory 2040-1 covers policies and procedures and suggests that: 'The form and content of written policies and procedures should be appropriate to the size and structure of the internal audit activity and the complexity of work.'

Audit Approach and Methodology

We are concerned with the manual as a projection of the audit personality or the voice of the director of auditing on the basis that, in practice, auditing can be performed in a variety of ways. The IIA standards recognize this issue and have framed their requirements in a generalized way with two main implications. First, differences in audit approaches and methodology are seen as inevitable and second, it is not enough simply to declare that a certain set of standards is being adopted. The precise audit philosophy must be agreed upon and documented for application throughout the audit department. The point that we are moving towards is that experienced as well as new auditors need firm direction on what is expected from them in terms of discharging the particular audit role. In this respect, the audit manual is the ideal device for placing the agreed-upon solution on record. Each audit department must offer a defined product that is the result of the 'contract' struck between audit and the organization. Views from the world of management consultants can provide an insight into the need to assume a suitable methodology and offer a differentiated product. The ability to engage in less structured activities and move freely from project to project can be developed with a carefully thought out methodology. This may be set out in the audit manual but not from the generalized set of audit procedures found in audit textbooks.

Impact on Creativity

There appears to be a direct conflict between the extent of direction and standardization that a comprehensive audit manual provides, and the auditor's professional autonomy. Both are essential for enhancing audit productivity. This conflict is akin to the perennial problem of reconciling managerial control and autonomy, where autonomy is defined as the freedom to succeed or fail. Auditors cannot perform if they are unclear as to what is considered successful performance while at the same time little commitment can be achieved within a bureaucratic straitjacket. Audit manuals must recognize this inherent conflict.

Building a Conceptual Model of the Audit Manual

This section builds a conceptual framework that promotes understanding of audit manuals. The manual is a device for formulating and communicating the audit role in conceptual, managerial and operational terms. We can make several firm statements:

- All audit departments have some type of audit manual although the contents may be dispersed and consist of un-coordinated items of guidance. According to our definition, manuals should cater for all types of relevant material. This requires a mechanism by which all published guidance can be collected and documented. The worst run internal audit section may still produce a manual by locating all memos that management has sent to audit staff in one file, along with a copy of standards. There is no excuse for failing to prepare a manual, even if a formal version is not possible.
- The manual should provide an avenue for establishing mechanisms crucial to audit performance ranging from quality assurance, standards, performance appraisal, methodology, approach, standardization, automation and generally controlling the audit function. The ongoing search for excellence should be reflected in additions and alterations to the manual as a vital process.
- If the manual is not carefully conceived, formulated, implemented, reviewed and maintained, it is difficult to see how an audit department can achieve successful service delivery.

The Three Main Elements

We would expect to see the following aspects covered in any 'adequate' audit manual:

1. **The management of internal audit.** We expect to see coverage of objectives, standards, code of conduct, structure, policies, strategic plans and control of the audit function. It is wrong to omit material on audit management from manuals.
2. **The operational aspects of internal audit.** This covers guidance on how the audit role is discharged in terms of planning, approaches, procedures, methodology, conduct and the techniques to be applied, as well as guidance on specific audit risk areas with related controls, and different types of audits ranging from assurance and consulting work through to fraud investigations.
3. **Administrative matters concerning the audit function.** This catch-all section would include matters such as time sheets, subsistence, timekeeping and absences, job descriptions, health and safety, data protection, and equal opportunities.

The Dynamism of Currency

The extent to which the audit manual is kept up to date is one measure of efficiency. Procedures must be completely relevant or they will not be complied with. If not:

1. It gives out signals that the manual is not considered important by audit management and lowers its status. The objective of the document is to reflect and reinforce changing best professional practice.

2. It is difficult to insist on compliance and auditors drift into their own interpretations of the audit role.
3. It becomes a procedures document held in a rarely used filing cabinet. Important new events that affect the future of internal audit will certainly be addressed by audit management. If they are left out of the manual, it sends the message that the manual is not meant for real issues. Dusty old rules on time sheets and travel claims may be held unchanged in the manual and we return to the old view of the manual as a set of basic administrative procedures.
4. It means newly appointed audit staff, particularly at manager level, will have no firm commitment to adopt the audit style and methodology or to view the internal standards before accepting appointment. Conflict may arise that leads to a disjointed and un-coordinated service. The role of the manual in pulling together the audit resource around professional standards is lost.

A continual appraisal of the manual to keep it up to date and vibrant requires a firm policy of resourcing this. This can only happen where the manual is seen as an audit product to be successfully accomplished and the task is built into performance indicators for both individual auditors and the department. Our model requires current material to be part of the dynamic process of directing audit resources effectively.

Using Models

It is difficult to devise models that can be used to evaluate audit manuals since the content of each manual is determined by many factors including the perceived function of such a document. The content, style, degree of detail and length of each manual will be influenced by:

1. How important the manual is, i.e. how much audit resources should it consume and at what level? The type and size of the audit function will impact on the profile it achieves and this should be decided on beforehand.
2. What functional model is most appropriate in terms of the manual being a compilation of reference material, a general framework for the audit department or a more comprehensive guide to managing and doing the audit? The level of detail must be established.
3. How prescriptive should the manual be, and how much autonomy should auditors have?
4. How far can audit formulate their own policies or must they adopt general organizational policies? The organization will have established clear policies in many areas such as staffing, promotion and training, and these will have to be recognized in the manual. In other areas audit may set their own direction. The business unit concept devolves many corporate roles down to local manager level. This may mean that the manual can set its own rules for auditors in the search for quality services.
5. Is it necessary to document all guidance or can we leave some matters in conversational mode where audit management makes decisions based on the individual circumstances of each problem? This can be easily catered for by inserting in the manual considerations such as 'audit management will determine the precise level of testing having regard to the circumstances of each case.'

Managing the Audit Function

Documenting management's decisions on how the audit function will be managed and performed will be reflected in the manual and will form the basis for strategic review. The principles in the

model are based on managerial concepts and derive from systems thinking. Some of the attributes of good audit manuals include:

- Objectives must be clarified. The point in a continuum should be selected ranging from a simple list of reference material, a general overview framework through to a comprehensive operational guide to controlling an auditor's performance.
- The contents of the manual, in terms of topics for inclusion and degree of detail, should relate to the need to fulfil the chosen objectives. This depends on the size and type of audit service provided.
- Standardized forms are advised and care should be directed to their design and use and the potential for automating the audit process.
- The adopted procedures and working papers should be based on the assumed standards in terms of ensuring that the requirements of the standards have been adequately discharged. It is not good practice simply to use forms and standards taken from other organizations' audit manuals.
- A clear audit methodology should be selected and applied based on the needs of the organization, the audit charter and the level of skill and experience of the auditors.
- The creativity and initiative of auditors will not prosper if their professional autonomy is curtailed. 'Auditing by numbers' is unproductive.

Applying the Conceptual Framework

The final product is not the manual but the successful implementation of standards and methodologies. We need to define and formulate a framework that incorporates the main principles behind successful manuals. The diagram in Figure 8.19 is based on four main planks of the audit manual process:

- The task has to be properly resourced (A).
- The wide concept of the manual has to be supported (B).
- The manual has to be used by auditors (C).
- It must play a role in evaluating auditor's performance (D).

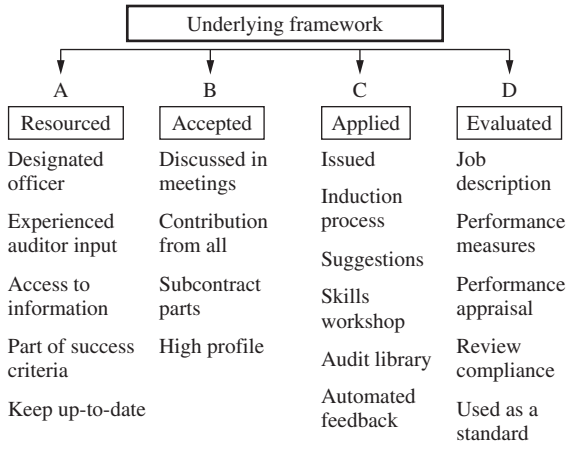


FIGURE 8.19 Framework for successful audit manuals.

Explanations follow:

(A) **Resourced** – An experienced audit manager should produce and maintain the manual.
(B) **Accepted** – The manual should be brought into mainline audit management and managers' meetings should include discussions on 'implications for the audit manual' for all decisions made. Parts of the manual should be subcontracted to auditors (mainly managers) and again this should be part of performance targets. The chief internal auditor should ensure that the manual maintains a high profile and is a constant discussion topic. It is possible to rotate the task of maintaining the manual between auditors and introduce an element of competition in improving it.
(C) **Application** – It has to be used by auditors based on understanding and acceptance. First, it is essential that all auditors have a copy and a process for inserting amendments. All new auditors should go through induction training based on the manual. Specially tailored skills workshops may be regularly held either internally or externally to cover separate topics in the manual on, say, flowcharting, systems-based auditing, report writing, statistical sampling, and interviewing. Convenience in design and use encourages auditors to keep their manuals close at hand and if PC notebooks are provided it would be sensible to hold the audit manual on hard disk. The ability to copy standardized working papers from the manual for use during the audit will feed into the process of automating the audit. Feedback should be obtained from auditors, particularly where there are inconsistent or difficult parts of the manual, along with suggested improvements.
(D) **Evaluation** – Auditors should use the manual to guide performance and quality assurance. The requirement to comply with the manual must be included in job descriptions and the manual should establish how performance will be measured. A formal performance appraisal scheme should be geared to meeting the standards set out by the manual. Supervisory review of auditors' work should look for compliance with the manual and audit managers have a major role. It is possible to use the manual as the standard for the performance of audit work and develop a career development scheme based on the manual. We might devise levels of ability to perform to the manual's requirements as shown in Table 8.3.

TABLE 8.3 Ability levels: understanding the audit manual.

Ability level	*Understanding of the manual*
Level 1	General understanding of the principles and techniques in the audit manual
Level 2	Comprehensive understanding of the principles and techniques in the audit manual
Level 3	Excellent understanding of the principles and techniques in the audit manual

The performance appraisal programme may be based on the requirements of the manual. This can be extended so that junior auditors fall at level 1 and senior auditors at level 2, and promotion to audit manager grade depends (in part) on achieving level 3 performance.

Selecting the Right Model: the Three Models

1. **Compilation of reference material.** This contains basic rules developed over the years governing audit staff. Managerial policies, operational concerns and other high-level issues would not appear.

2. **General framework for the audit function.** We move now to a more developed format where the manual sets frames within which the audit work is contained. The approach to planning, systems-based audits, reporting and so on will feature in this version of the audit manual. The guidance will be in outline form that will set general policy rather than finer detail.
3. **Comprehensive guide to audit work.** This seeks to cater for most of the situations that the auditor will experience. The proactive use of standardized documentation and checklists is the main feature. The manual will be self-contained in that it should include material that the auditor will require on a day-to-day basis. There will be extensive reference to documents in the audit library and the network.

Other Factors

These include the type of auditor employed and the size of the audit function. More guidance is required where auditors are less qualified/experienced or in a large audit department. More experienced auditors can be given more autonomy than those less experienced. This can be highlighted in Figure 8.20.

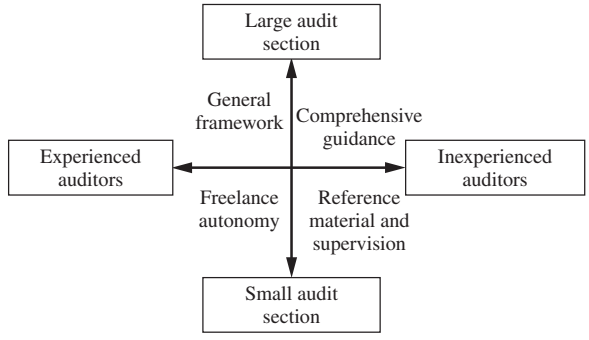


FIGURE 8.20 Impact of the number and type of auditors.

Overcoming the Creativity Problem

There is a contradiction in the underlying objectives of the manual in providing direction throughout the audit function, and the need to maintain professional autonomy. The greater the degree of guidance provided, the more the auditor's efforts are restricted by standardized audit procedures. It is necessary to reconcile the two opposing forces of autonomy and control. The model in Figure 8.21 sets out the relationship between these two main factors.

The point that we must arrive at is where auditors retain their professional flair and imagination but direct effort in the way that is required by the chief internal auditor, in line with the existing audit strategy and organizational culture. In this way, we would move towards the target position shown in the far right-hand corner of Figure 8.21 by developing the 'professional auditor':

1. **Ensure that more comprehensive guidance is only provided where it is required.** Consider, for example, the scenario where a particular methodology is required rather than a basic textbook approach. It is not necessary to cover common-sense points that the auditor will know anyway. We will seek to concentrate more on areas where there are different options that the auditor may adopt, and so promote a degree of consistency.

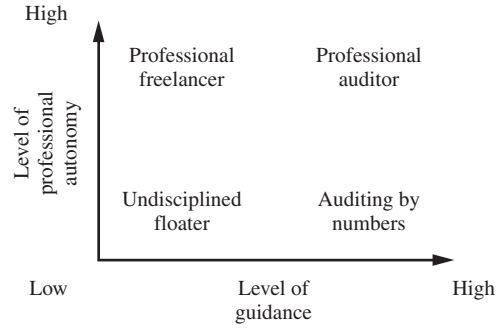


FIGURE 8.21 Autonomy versus control.

2. **Leave general reference material outside the main audit manual.** We may make extensive references to the audit library and documentation published by the organization itself. These factual matters can be explored at leisure without clogging up the manual with unnecessary detail. At times, it may be necessary to repeat pointers from key documents such as the purchasing code of practice. Here a brief summary of limits and rules may be mentioned and reference made to the full document which will be held in the audit library.
3. **Indicate whether a particular procedure is optional.** It is good practice to state clearly where auditors are expected to carry out certain defined routines in contrast to those parts of the manual for guidance only. A suitable code may be applied (e.g. bold or set in a box) to make this clear. Where it is possible to leave matters to professional judgement, then this approach should be pursued.
4. **Explain why a procedure has been selected.** Resistance arises where an auditor does not feel it necessary to follow a rigid routine. Explanations can help break down this barrier by demonstrating why it is required. For example, if we insist on the manager signing each working paper when it has been reviewed, this potentially cumbersome process can be justified as part of the quality assurance practices. If auditors are required to note (in their diary) any decisions they have made over the telephone, again the reason may be stated.
5. **Allow departures as long as they are documented and justified.** We can avoid treating people as children by setting standards that allow some discretion where required. The terminology used can promote this approach by allowing departures in defined circumstances. The key is to encourage some discretion while stopping all-out anarchy, by careful drafting of the audit manual.
6. **Encourage all auditors to participate in improving the manual and consider rotating the task of maintaining it.** The manual should develop from within the audit function and not be imposed from above (or outside). This will bring some degree of consensus and involvement into the process of establishing and maintaining the manual, and thus generate a feeling of teamwork. This is in contrast to an elitist approach where the manual is given to a 'high flier' for development as a form of wholly theoretical model building, far removed from the practicalities of working life. Note that this is just as bad as giving the manual to an administration officer and so lowering its profile.
7. **Do not appoint an auditor until the approach and standards are explained and he/she can work within them.** We may place the requirements of the audit manual in front of newcomers before they sign the formal contract of employment. Our model suggests that the manual will be a detailed document that creates many demands on senior and junior auditors as they strive to meet the high professional standards embodied within

the audit manual. This position should be made clear to all persons who are considering an offer of employment as we will require full commitment from staff. This 'opt out clause' may save discontent as new staff feel unable to work within the confines of comprehensive managerial and operational standards that they may be experiencing for the first time.

8. **Where a requirement in the manual has been overridden consider whether an amendment is required.** The most frustrating feature of the audit manual is where elements are no longer appropriate or lead to unnecessary work. Non-compliance can be deemed to be a basic breach of procedure or indicative of a problem with the manual itself. The first port of call is an assessment of the adequacy of the manual, particularly where the breach is frequent and spread across the audit function. Unrealistic parts of the manual must be removed or revised and this is a matter that should be under constant review by the CAE.
9. **Ensure that auditors who refuse to perform to the requirements of the manual are moved out of the audit department.** The approach adopted above was to stand back and consider the manual in the event of non-compliance. After this issue has been dealt with, we will turn our attention to acting on unjustified breaches of audit standards. This is a simple matter and requires audit management to reprimand the culprit immediately when a problem arises and seek dismissal where there is continual or serious case of non-adherence. As long as the manual has been properly drafted and implemented, nothing short of this action is required to retain the credibility of the manual as an important management tool.
10. **Test each section that is drafted to ensure that it is not unnecessarily cumbersome and bureaucratic.** Nothing should enter the audit manual until it has passed the 'sensibility test'. This requires a considered process whereby the proposed changes are dealt with by audit management and reviewed in detail before they appear as a formal revision to the manual.
11. **Watch out for auditors who appear demotivated and investigate underlying reasons.** Where staff are demotivated and/or seek resignation, we must find out if this is the result of inappropriate auditing procedures. Group meetings may highlight this problem as will exit meetings for auditors who leave.
12. **Ensure that there is a continuous programme to search for and amend all faults.** We should keep a watchful eye on anything that impacts the manual. It is as well to make the audit manual a part of the agenda on all audit management meetings that address developmental issues.

Structuring the Audit Manual

As with other features of a manual, the structure and content depend on the particular circumstances, although it is possible to set out a four-tier model for structuring the manual as in Figure 8.22.

1. It is generally better to have a few main sections as with the model in Figure 8.22 so as to generate some degree of form and structure. Accordingly, each main section should have a focus that sets the tone for the material that it contains.
2. Keep basic reference material outside the audit manual. Reference material can consist of many pages of detailed information that is generally applicable to the staff of an organization. Auditing standards, on the other hand, deal with professional approaches to discharging the audit objective, which should be the main thrust of the manual. These two types of guidance should be differentiated and, as we suggest, the former is best held outside the main body of the manual.

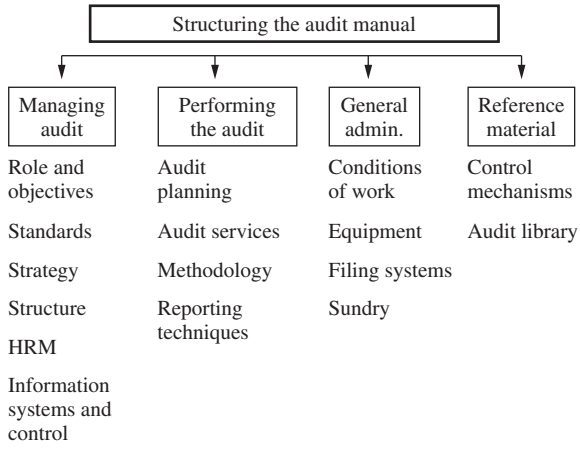


FIGURE 8.22 Structuring the manual.

3. Maintain an extensive up-to-date audit library and cross-reference this to the audit manual. The audit manual should contain a list of contents of the audit library and an indication of other relevant material held elsewhere. This standard, however, depends on a comprehensive library that meets the requirements of most day-to-day audit work, as a considered investment. The library complements the manual as the manual will act as a funnel that invites the reader to explore useful detail held outside the manual. In short if the manual is to work, the library must also work, which as a resource issue must be fully funded by the CAE. Information may also be held on the audit database.
4. Ensure that all the topics mentioned in Figure 8.22 are fully dealt with in the manual so as to promote a complete and worthwhile document.

Note that the relevant material may be held on CD or the network.

Implementing the Manual

The process of formulating and implementing a new or revised audit manual is shown in Figure 8.23.

We hope that the resulting manual would be linked to the audit strategy, which in turn is based on the organization's need. In addition, it also takes account of the specific needs of the auditors as well as the chief internal auditor's views on the way the audit role should be discharged. Lastly, it is hoped that after developing the auditors to enable them to apply the methodology and techniques as required by the manual, they will in turn be appraised in accordance with their success, or otherwise, in this task. The implementation process should include skills training workshops that explain and expand upon the contents of the manual as an ongoing process. Desk (on-the-job) training seeks to bring the manual to life by relating it to the actual work that is being performed. The onus is on audit management to have much expertise in understanding and applying the requirements of the audit manual. The other key point is to try to assimilate the audit manual into formal managerial mechanisms such as audit strategy, performance appraisal,



FIGURE 8.23 Implementing the audit manual.

marketing, quality assurance routines and so on. Where this is successful, the manual will perform its main role in providing the very foundation of the audit service.

Maintaining the Manual

It should be a dynamic mechanism for directing auditors and as such it is ever-changing to reflect the latest circumstances and strategy. Accordingly, there should be regular changes either adding to the material in the manual or amending sections, and all should participate. A useful technique used by one audit department provides that whenever an auditor attends a conference or training session, he/she would give a brief presentation to the audit department and draft a summary of any relevant matters for inclusion in the manual. One would imagine that the manual might be updated/amended every week and weekly or bi-weekly staff meetings might be a good forum for this process; in addition, quarterly comprehensive reviews might also occur. It should be a constant challenge for dedicated auditors to keep up with the manual and we would expect audit management to acknowledge those who undertake this task successfully. The culture of audit should be such that it becomes a compliment to be asked to be responsible for the manual and this could be rotated, say, quarterly. Most of what happens that impacts on the auditor's work should also be deemed to have an effect on the audit manual. If this principle is applied as a rule, we should see no problems with maintaining the manual in the fullest sense of the word. The chief internal auditor has a clear responsibility to provide formal guidance and direction to auditors and if this is not done, audit can become an un-coordinated, undisciplined affair relying on word-of-mouth and isolated comments from audit management. Research has shown that the audit world does not generally assign a high profile to audit manuals and they have been somewhat neglected particularly in the 1990s. If we are prepared to commit resources, build supporting frameworks and consider the potential role of the manual, then many models can be devised to assist in promoting the manual as a vital control mechanism. Where the CAE is not wholly sold on the idea of using the manual as the key managerial control, then nothing will be achieved via this document. One final point to note is the inherent hypocrisy in commenting on an audit client's failure to establish suitable operational procedures as part of the control systems that have been audited, especially when the reporting auditor is not able to point to a sensible audit manual that performs this very role for the audit service.

8.6 Delegating Audit Work

Audit management should delegate work to more junior staff. This can be a powerful way of not only increasing overall efficiency but also developing auditors. There are pros and cons, although delegation needs to be understood and controlled.

The Delegation Process

The delegation process involves conferring authority to perform defined tasks. The overall responsibility remains with management, who is accountable for the outcome. One view of delegation is shown in Figure 8.24.

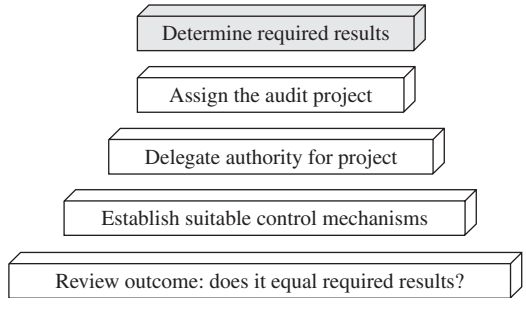


FIGURE 8.24 The delegation process.

Delegation in Internal Audit

We differentiate between technical and practical delegation. In technical delegation, the CAE is ultimately responsible for the activities of the internal audit department. Audit managers are likewise responsible for the activities of staff under their control. Delegation allows auditors to perform the day-to-day work unimpeded, around audit plans where each internal auditor has defined responsibilities. A restricted definition of delegation is when what are normally management tasks are given to auditors in addition to, or in place of, their normal workload. These extra and more demanding tasks/projects must be carefully controlled. An example is the audit manual whose maintenance is the responsibility of the CAE but may be assigned to an experienced auditor. Other examples are:

- Audit brochures
- The annual report
- Special projects
- Quality assurance programmes
- Auditing standards
- Marketing logos and web-based material
- Client presentations
- Internal reviews of audit files
- The audit charter
- Staff training and development

Delegation is not abrogation of responsibilities. The CAE must be involved in matters that have a major impact on the audit services and delegation must be used with care. This includes sensitive

topics such as confidential audit marketing plans, managing the audit budget, auditor discipline, the audit committee, material complaints against auditors and reviews of audit strategy. Advantages are the positive effect on staff and getting work done. The key benefits are:

- Auditors may be able to do a better job than their managers.
- Auditors themselves learn to delegate.
- New ideas may be generated.
- It acts as a communication device between managers and staff.
- It promotes trust across the internal audit department.

Delegation forces management to set clear objectives and define scope. Senior auditors may spend hours on an obscure project that provides no end product. Delegation creates the drive for the audit manager to define and communicate exactly what is to be achieved. It must be based on trust between parties each with differing needs (Table 8.4).

TABLE 8.4 Manager/subordinate requirements.

Manager	*Subordinate*
Wants good results	Enjoys the challenge
Wants to look good	May make mistakes
Wants to save time	Needs support
Wants no problems	Wants it to work out

The audit manager must allow for mistakes and this is part of letting go of some managerial authority. Management should reward increased performance in taking on more difficult work. Delegation stimulates enhanced performance through opportunities provided. Problems result where additional pressures create stress and lower the auditor's ability to live up to the challenge. It is better to use the extra effort to accelerate progress of the auditor's career development, which is why a policy on internal promotions can be useful. There must be real benefits.

Barriers to Delegation

Bad experiences may remain in the manager's mind where a task has been entrusted to someone who has not delivered. Internal audit should charge for each hour spent on client projects and if time has been misapplied and a project is unsatisfactory the client may not pay. The remedy is to isolate the problems and ensure that they will not occur again. This is simple as long as the manager is professional enough to admit to mistakes. Professional jealousy arises where the CAE or audit management will not allow staff to shine. At its most destructive, the CAE refuses audit managers access to corporate management. All work is reported directly to the chief executive and senior directors and is personally performed by the CAE. Work builds up, and the CAE has no time to manage the audit function. Backlogs arise and emails are left unattended while the CAE tries to impress the management by insisting on personally carrying out sensitive, confidential projects. This derives from the CAE's insecurity and mistrust of their staff. Other barriers include:

- untrained junior auditors
- inability to understand the delegation process

- lack of time
- insufficient work available to the audit manager
- competition from subordinates
- fear of losing control.

Establishing Control over the Delegating Process

Auditors have no excuses since the audit review process requires clear objectives, time budgets and quality standards. Control arrangements include those in Figure 8.25.

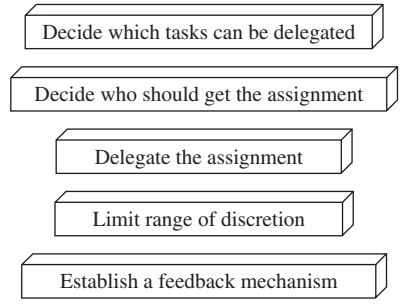


FIGURE 8.25 Controlling delegation.

Each stage should be carefully thought about by audit management who must ensure the right work goes to the right staff and there is a continuous check over progress. This is over and above the day-to-day audit work within the normal scope of work for the grade of auditor. An example will help:

> The CAE realized the audit manual was out of date. The task of updating this was given to a senior auditor who had just passed professional examinations. This person was interested in auditing procedures and newly published material collected during studies. A budget was given and precise terms of reference discussed with the CAE, audit manager and auditor. As and when each section was produced, it was reviewed by the CAE before the next one was started. A weekly meeting was held with the manager and auditor to discuss the progress. Hours charged to the job were carefully monitored.

Discussion, objectives and scope, time budgets, quality standards and frequent information all enhance control. Motivation, career development and encouragement from audit management add to this ability to direct and control tasks assigned to staff. There is a final point to consider regarding the degree to which delegation is applied (Figure 8.26).

Delegation is accompanied by directions and may involve assigning a complete job along with associated decisions. At the other extreme, it may entail the simple task of obtaining information and handing it over intact to the manager for interpretation and further work. There is no reason why delegation should not be employed to the full.

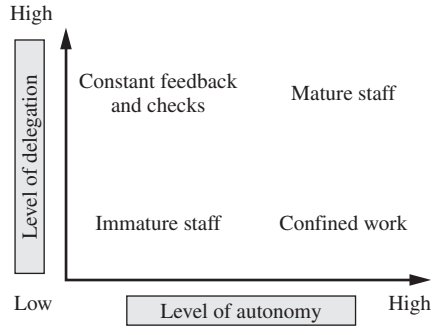


FIGURE 8.26 Levels of delegation.

8.7 Audit Information Systems

The computer has major implications for audit work. Effects range from impact on the audit field to the way audit work is performed to how audit itself uses computers to improve productivity. This section provides an introduction to the impact of computers in developing internal auditing strategy (Figure 8.27).

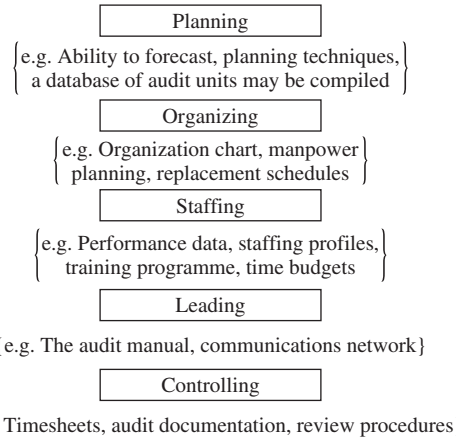


FIGURE 8.27 Impact of information.

Management should undertake a constant search for ways that information technology (IT) can be used to improve the audit service. This may mean employing computer personnel to promote IT skills through the department. An information systems strategy should be developed to ensure that efficient information systems are developed to support the overall audit strategy. The strategy should also be geared into developing overall computer literacy so that auditors may be confident in the way they approach automated systems. This may allow a step into computer audit whereby advanced computing skills may eventually be acquired. Public systems such as the Internet may be accessed and form an almost limitless database of reference information. In-house information databases may be built up over time as a complement to the audit library. In fact, it is difficult to explain how an audit department could prioritize systems-based auditing without developing a

database on available control mechanisms. Direct information links between the auditor and the audit office can arise via the PC notebook, which can send data to the audit-based terminals. It is then possible to promote the freelancing auditor whose motto is 'Have notebook, will travel.' Furthermore, time-monitoring systems can account for audit hours and be linked into a planning and control system. In addition, they can be used as a billing and accounting system.

The Development of Information Systems

Part of an internal audit management's task is to formulate and install a suitable information systems strategy and here we cover some of the matters that should be addressed. It is possible to set the terms of reference for computer audit to include responsibility for assisting with this information strategy as part of their everyday work. The use of in-house information technology staff to support IT initiatives should also be considered in line with the fact that auditors are also IT users. There are a number of strategies that the audit manager may adopt including:

No impact Here IT is not seen as an important resource and a no-development strategy ensues. This will mean that machines will be replaced as and when they break down, no budget for IT will be secured and there will be little or no development in the type of software used in audit work. This position occurs where there is no one person given designated responsibility for IT development and it is therefore not seen as important.

Automation in current form A more progressive strategy appears where audit management seeks to automate existing activities by the application of new and/or enhanced IT. Audit management may ask basic questions such as:

> How can IT help us perform our existing functions in an automated fashion?

Greater development will arise where management optimizes activity through greater levels of automation. These strategies are still confined by the consideration of IT's application to existing activities.

Enhance functions performed by activities Higher planes of performance can be achieved where audit management asks:

> What new functions can be performed through use of IT to promote achievement of audit objectives?

What may be seen as the final phase of IT assimilation occurs where we seek new activities through the use of new technology. Existing applications may be reconfigured into an 'audit IT network' where shared information enhances communications throughout the audit function. New audit tasks such as matching and merging different systems databases can be developed as an aid to management in ensuring the integrity of automated information. This format is, however, wholly dependent on the continuing search for new and improved systems for use within the audit function, which in turn is dependent on resourcing this initiative. One such role fundamental to this objective is the ongoing study of newly released software that brings an ability to perform

more powerful functions. Software is now becoming more flexible, user-friendly and integrated. Taking advantage of these developments is a major task that requires the implementation of the process (Figure 8.28).

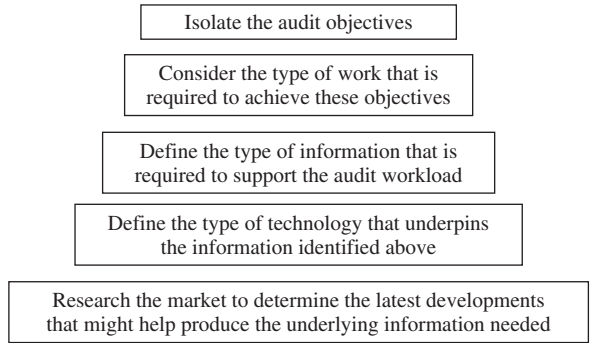


FIGURE 8.28 Using IT developments.

We must not only understand the audit role and types of work products that support this role but also appreciate how new IT can fit into this scenario. New releases of software represent new systems and it is these systems that are important. The operating systems and environment simply support the systems and again represent a major purchase decision. Unfortunately, many newer systems require a certain type of environment (e.g. the latest version of Windows). The machines may, in practice, be seen merely as potential obstacles in terms of providing the skeleton upon which the system sits. The problems arise where the machines are not fast enough, powerful enough or have insufficient RAM and/or hard-disk capacity. Audit management must ensure that the machines keep pace with the systems and in this context 'upgradeability' will be the buzzword. We must keep an eye on other business units within the organization to ensure parity in IT development.

IT as a Strategic Resource

We are moving closer to the concept of IT as a strategic resource for the internal audit unit. The key questions asked by audit management become more urgent and will be framed more in terms of:

> What are others doing with IT? Have we got state-of-the-art printers? Are we fully into desktop publishing? Have we got an edge on similar audit units? Are the external auditors ahead in the IT stakes? Can we download, manipulate, analyse, utilize and maximize our use of organizational databases? Is there anything else we should be doing? Who should I be talking to?

Strategic IT considerations must move to a high level where major related concepts are addressed at audit management meetings and reported regularly. These matters will include:

Added value We would expect the investment in new IT to add speed and vitality to the work product and so increase the overall value of the audit service. IT does cost a lot and needs replacing regularly as new software makes increasing demands on machine capacity.

Competitive position What is done elsewhere should be done in internal audit and the idea of 'keeping up with the Joneses' applies in this environment. This is particularly appropriate for presentation purposes and database interrogation. Where parts of the organization are producing colour reports, we must also consider our position in this regard, so as not to be left behind.

Better information New IT is primarily about getting better information and this must be an important consideration for audit management. For example, our time-monitoring system may be outdated and not able to provide a sophisticated package of reports as well as providing a client-charging system. IT is not only about buying in improved facilities but should also act as a stimulus for considering the adequacy of existing information and how it can be improved.

Cost containment Information is about improved services as a result of better decision-making abilities. Another concern is the possibility of reducing the costs of the audit service in terms of reports produced. The biggest audit cost is time charged to jobs and it is here that we would expect vital information on weekly charging profiles to contribute to the task of keeping these charges contained within budget. Exception reporting is applicable to audit as well as other parts of the organization, and this should direct the CAE to key areas of concern that may be falling out of control.

Managerial effectiveness We have set out a number of performance indicators applicable to internal audit earlier on. The information systems that are used by audit should be geared to furnishing the required feedback for each of the key measures. For example, audit management should be able to tell how many reports have been issued, how may audits have been aborted, how many audits are over budget and so on in line with the adopted performance measures.

Link back to head office We should develop the communications model where auditors are able to plug into corporate systems from anywhere in the organization (or from home). The main consideration for audit management is the need to keep sensitive information confidential.

Better flexibility Having the ability to set vast databases of reference material onto audit notebooks can create a real freedom from the paper-based environment. This added flexibility should contribute to the efficiency of the audit service as a major benefit.

Real time working The move from past data (say many months old) to on-line up-to-date information can have many benefits in terms of the vibrancy of audit reports. The ability to address current data as part of our audit findings moves us from the past into the present-day environment.

Better control An overall improved state of control can be promoted through increased use of new information technology. This is an important consideration as the internal auditor may be seen as the in-house expert on internal control.

Data is a resource that makes a vital contribution to service delivery. Being at the front of this development is important. Some time ago, the IIA has issued a Professional Practices Pamphlet (98-3) on automating the audit workpaper process that contains the following key extracts:

> The IS auditor does not lose independence by performing tasks such as:
>
> - Reviewing controls.
> - Testing compliance with standards.

- Providing advice on control techniques.
- Promoting the use of project management.
- Determining whether security standards are sensible.
- Advising on the management of systems performance.
- Helping management identify and address relevant risks.
- Helping to identify project roles.

Audit workpapers must permit any experienced auditor having no prior connection with the audit to follow the audit's flow and support the auditor's conclusions. While the Standards do not refer to automated workpapers, one may infer that auditors must structure automated workpapers in the same manner as written hard copy workpapers. It is of the utmost importance that automated audit techniques used in audits are properly documented, understandable, and reliable so that any experienced auditor may review audit workpapers and follow the results of an audit performed using such techniques.

Resourcing IT

The costs of new IT can be great and it is commonplace to buy in new systems only to find that they have become obsolete, with new and improved facilities on the market. This constant struggle to keep up with new technology can be frustrating, which is why our policy must be derived from a clear vision. This vision should drive and direct the CAE towards a constant search for excellence. It may be based on establishing a paperless environment, whereby paper files are frowned on and manual working schedules are positively discouraged. The relevant model is shown in Figure 8.29.

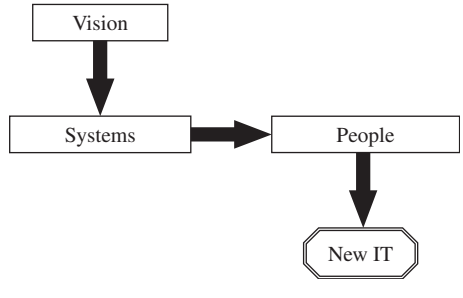


FIGURE 8.29 Translating vision into reality.

Audit management must set aside time to develop this vision and ensure it is filtered down into control systems, how auditors work and the necessary facilities (IT) to support this model. A clear vision is derived from talking to stakeholders about their expectations and developing a value-based foundation of words that action (and auditor competencies) may be built around. The next question to address is: What information is required to support this vision? The greater the impact of IT, the greater the level of resources set aside to buy in the new facilities. Where this impact is deemed material, we need to implement a system's architecture in support. This architecture should cover the entire audit function and all existing computer facilities and new requirements in a programmed manner. It is here that we may arrive at a global solution to cover the whole audit unit. The vision we speak of is more than a general statement of intent but is a work-based condition that looks for progress in all fields of work. In terms of the application of new IT, during the course of a working day, the CAE may ask basic questions such as: Why

are these files lying on desks? Why are we still preparing manual spreadsheets? Why are we not downloading data from the corporate personnel system? Why are we not producing colour graphics in our brochure? Why are we still sending audit reports to the print shop? Why does this auditor not use a PC?

Hierarchical Structure

When developing suitable information systems, we must take an overview in considering the precise information requirements of internal audit. It is amazing how many IT development projects are formulated without a system analysis. This process should ideally utilize a top-downwards approach where we start with a 'big picture' before moving down through the function to isolate where IT is best located. The starting place is important, in that it sets the tone for the rest of the exercise. Physically we start from the CAE, through audit management and work downwards, while conceptually we must start with the basic process (Figure 8.30).

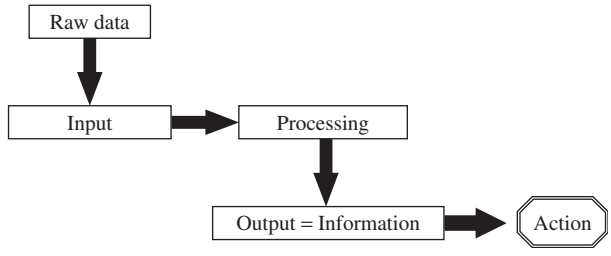


FIGURE 8.30 Generating useful information.

It is the action that is important since information is of little use unless it is converted into a suitable action. This brings into play the second problem with many IT developments where there is no full recognition of the types of actions that management must pursue in furtherance of audit objectives. This is why it is best to generate the project internally through audit staff (say the IS auditor) as opposed to external consultants. The final view of information is one based on the type of action that it is meant to stimulate, which may be classified in the following manner:

Strategic Audit management requires aggregate information, say monthly, that sets the global position over the entire audit function for long-term planning. This 'big picture' will assist in the overall direction of audit and help develop a futuristic strategy to cater for the next few months or years.

Managerial Weekly time sheets, if processed properly, will generate weekly reports that may be used to get a fix on the performance of audits and auditors. These reports will be more detailed and give the narrow and more accurate picture that is required to make quick decisions on resourcing all current audits. We may wish to abort audits, extend them, transfer resources and/or seek explanation from the field auditor on receipt of this type of information as part of the management process.

Operational Daily feedback on what is going on in internal audit is one way of controlling resources. This may be related to information on who is doing what, where, for how long and why, so that relevant decisions may be made as required.

Attributes of good information are:

Timeliness	Documented
Effectiveness	Flexible
Security catered for	Efficiency
Accurate	Accepted
Quantity	Relevant

Audit management would be advised to review the reports they receive to determine whether they adhere to the above-mentioned standards. Bearing in mind the emphasis we have placed on the importance of information as opposed to IT, we can list here examples of some of the reports that will typically be prepared by internal audit for use by audit management:

- summary of reports issued and findings
- summary of chargeable hours to projects
- breakdown of non-chargeable hours such as general administration
- summary of auditor performance appraisal reports
- level of sick leave and other absences
- current status of all outstanding audits
- audits over their time budget.

An IS Strategy

When devising an IS strategy for the internal audit unit, there are a number of matters that should be given due attention:

- Rooted in business strategy. The first point to note is that the information solutions must be based around a clear business strategy if they are to have any use at all. This means that the CAE needs to formulate a clear plan of action to cater for the next few years to drive the audit service forward. One key matter that should be addressed in this respect is whether the CAE is seeking fresh markets in line with an expansion policy. The converse is where audit wishes to become 'lean and mean' in preparation for being more competitive, and so intends to release staff over the coming months. The position of IS audit will also have an impact on the IS strategy where we may choose between centralized computer audit teams or devolved models where all auditors are deemed IT literate. Again the type of facilities applied will depend on the adopted model.
- Prioritize applications. Part of the IS strategy will be based on the determination of the types of systems access that are required by the auditors. In general, we would want all auditors to have on-line access to all key computer applications run by the organization. The way this is brought about should be firmly built into the IS strategy.
- An effective IS strategy will tend to take a global view of the main considerations that are required to progress the audit service in the information arena. In one sense, we are required to make information a high-profile issue as it forms the lifeblood of the audit service in the way shown in Figure 8.31.
- The solution should be seen as an entire package, which will take on board factors such as audit plans, the IT budget and IT standards.

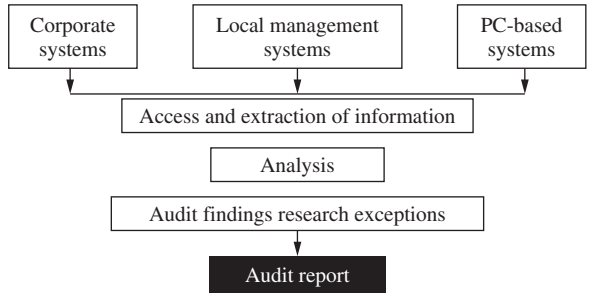


FIGURE 8.31 Information needs of audit.

- One of the most common failings of audit management is an approach to IT developments that does not recognize that a formal project is actually being established. An organic approach to IT has the advantage of ensuring resources are attracted to areas of most need (or people with the loudest voice). The setback is the absence of the important controls that appear over projects. These controls involve defined resources, deadlines, specific products and tasks, regular review, monitoring reports, documented meetings and so on. Auditors are excellent at auditing defined parts of the organization but sometimes fail to install in their own section the very controls that they recommend elsewhere. We will spend a great deal of money on IT and this will probably be the next most significant item of expenditure after staffing costs. It is a fundamental part of audit management's responsibility to install adequate controls over this expenditure.

The Importance of People Involvement

There are many people who have a role in IT development and who will have an opinion on the types of solutions required. This will include corporate IT officers, hardware suppliers, consultants, computer audit, field auditors and even the auditee (who will promote their own systems). The CAE will reconcile these competing influences and work out who is offering the best advice. It is good practice to pass all proposals through audit management meetings. People give different advice, and there are many reasons why certain systems are supported by certain people. Some of the 'people considerations' that relate to IT can be listed:

- Human resource planning is required to ensure that auditors have the necessary skills to administer the systems that are required to discharge the audit role. We need to consider training needs, staff development and the way audits are undertaken. Computer boredom is an additional concern where it is not always easy to get staff to use new systems unless they are motivated. It is as well to have a requirement that auditors use new IT built into job descriptions in case there is some dispute in this matter (in terms of cooperation).
- The other side of human resource planning is a more proactive approach where we need to fast-track the required skills by considering interactive training (CD based), recruitment policies, scarcity allowances, redeployment, redundancies and dismissal where the skills are not present.
- The final side of the equation is the power play that comes with new IT. Resources may be deemed to relate to the level of status of the officer in question. So, for example, instead of resources being allocated to staff on a needs basis, they will be assigned on the basis of grade. Unfortunately this is part of human nature, which can result in the misapplication of IT resources.

Time Monitoring Systems

Time management system will tend to feature in most internal audit units and this will be an important information-based system. This should enable audit management to receive regular reports on the way their staff are working. It will be used to support performance measures that relate to a variety of performance targets that would ideally have been set for both auditors and audit teams. They should cover each of the defined information needs that derive from the management of audit time. This will involve periodic reports as well as specially requested items. The reports should revolve around the time frame, types of work, auditors, audit groups and the entire audit unit. As such, it should report on:

- time spent on audits;
- audits over budget;
- non-recoverable time charged (such as training);
- breakdown between systems and investigations;
- audits that should have been completed; and so on.

The inputs of a suitable time monitoring system are illustrated in Figure 8.32.

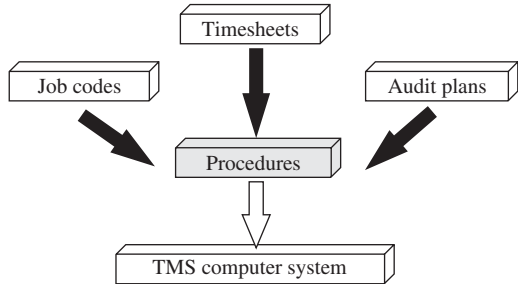


FIGURE 8.32 Time monitoring system inputs.

The various roles of time management information should be duly recognized and catered for. Here, we would expect any such systems to cover the following functions:

1. A method of charging time to specific audit jobs.
2. A way of identifying variances from planned to actual hours through incorporating budgeted hours to each chargeable job.
3. A method of charging clients for work carried out and generating the supporting schedules and covering invoice if needs be. Accordingly, it is important to identify a client for each job that is set up on the system.
4. A method of establishing the status of each job. Suitable booknote messages may be used in any good system to compile a form of database of audit jobs, which will provide summary information. This may range from terms of reference, assigned auditor, special features, stage indicators (say planning, field work or reporting) and so on.

The time management system will typically be a computerized package that performs the function of recording and reporting auditors' time. There are three main components that must feature in

the system for it to work. This is the auditor's weekly time sheet, the job coding (and clients) and the planned hours. This may be illustrated in Figure 8.33.

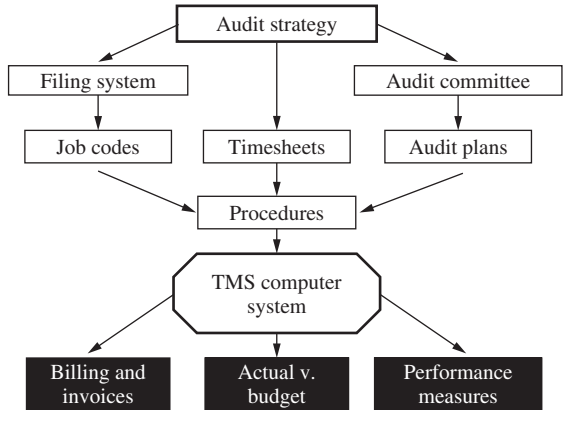


FIGURE 8.33 The audit time monitoring system.

As such it is not just a matter of buying a time management system and installing it on a PC or network. The underlying procedures must be carefully thought through and addressed before a suitable reporting system can come on-line and be of any use to audit management. Building on the point mentioned above, it is as well to resource any time management work as a proper systems development project. Here the task is not just left to the audit administration officer but is assigned a high profile and given the status of a formal computer project. To this end, for larger audit units, we may designate the following key officers:

A systems controller This might be a senior auditor who would be responsible for job code structures, technical detail on the system including archiving, data input standards, enhancements, and rules regarding who has access to the system and how the integrity of the database is maintained. This person may have to write procedures for time sheets, the input data and reporting functions.

A systems manager This may be an audit manager who will have overall control over the system and set the general strategy for its use, review, procedures and the way staff interface with it.

An input officer This may either be decentralized, with each auditor inputting their own figures (with controls over accuracy, say, managerial review of figures), or one person may hold this responsibility.

The data owner The CAE will have overall responsibility for ensuring the data are correct, the reports are adequate and the system is sound. The systems manager would be required to provide assurances on these and other related matters.

Again time management will not work if the role is simply delegated to the audit support officer and nothing more is done. It should be a regular feature of audit management meetings and a

key concern of the CAE. We have suggested that the job code structure is seen as a separate consideration before the computer system is established. Ideally this should reflect the way the systems-based approach and investigations role are perceived in terms of audit work and audit consultancy, respectively. Any coding system must be based on clear rules that will vary between different audit sections. We may, however, make some general observations:

1. Code the work in line with the adopted reporting framework. The audit committee may have a view on this. In this way, we may secure reports that feed naturally into our monthly, quarterly and annual reporting structures.
2. Do not allow auditors to set up individual codes for small jobs as this makes the system overloaded. A general code of 'advice and information' may be used to record these one-off tasks. We may set a time standard and require jobs under, say, one or two days long to go to this code. If this approach is adopted, it is important that time sheets record full details of the work and are retained for later review, if there is a query from the client.
3. Following this line, it is as well to have small number of fixed codes for non-recoverable (or non-chargeable) time such as annual leave, training, sickness and so on.
4. Have strict rules on who can set up codes and budget hours. This should be restricted to senior staff (say audit manager or the CAE in smaller audit units).
5. Ensure that time sheets are signed on a weekly basis by audit management before submission to the system.

We may set out an example of a coding structure where systems and investigations work have been separated (Table 8.5).

Managers rely on the progressive use of information technology and this means more computerization. This is also true for the internal audit department and suitable standards must be applied for controlling these developments in line with organizational policies. Automation is a fact of life and the audit department must have the same level of controls that it expects from the departments it audits.

8.8 Establishing a New Internal Audit Shop

Legislation and/or internal pressures can lead to a demand for internal audit where this has not existed before. Calls for enhanced corporate governance can make secure systems of control an organizational issue to be addressed through establishing an audit committee. Research has shown that the audit committee, even where primarily concerned with external audit, will mature and concentrate more on internal audit. The situation where a newly formed internal audit function has to be developed is not unusual and we cover this. Issues include:

The audit charter
The code of conduct
Training
Computer audit
The use of systems-based audits
Probity work
The audit manual
Service level agreements
Structures
Audit standards
Recruitment and selection
The business risk assessment
Fraud work
Business planning
The IT strategy
Audit services
Budgets

TABLE 8.5 Job coding system.

Description	*Job code range*
Recoverable	
A. Assurances – systems	
1. Corporate and operational	1,001–1,500
2. Financial systems	1,501–2,000
3. Systems development	2,001–2,500
4. Computer audits	2,501–3,000
5. Risk management	3,001–3,500
B. Assurances – investigations	
1. Management investigations	3,501–4,500
2. General probity audits	4,501–5,500
3. Fraud investigations	5,501–6,500
4. Other investigations	6,501–7,000
C. Consultancy services	7,001–8,000
D. Audit professional advice	(8,001–8,020)
1. Department A	8,001
2. Department B	8,002
3. Department C, etc.	8,003
E. Non-recoverable	(8,021–8,041)
General management	8,021
Audit admin.	8,022
Audit strategy, plans and risk appraisal	8,023
Activity reports	8,024
Client relations and marketing	8,025
Audit meetings	8,026
IT strategy and enhancements	8,027
Seminars, etc.	8,028
Professional training	8,029
IT training	8,030
Non-audit training	8,031
Other training	8,032
Delivery of training	8,033
Staffing issues	8,034
Recruitment of auditors	8,035
Performance appraisal	8,036
Audit manual, procedures and quality assurance	8,037
Audit library	8,038
Liaison with external audit	8,039
Non-audit work	8,040
Other	8,041
F. Absences	(8,042–8,049)
Annual leave	8,042
Sick leave – certificated	8,043
Sick leave – uncertificated	8,044
Hospital, doctor and dentist	8,045
Bank holidays	8,046
Special leave	8,047
Unauthorized absences	8,048
Miscellaneous	8,049

Main Considerations

1. The audit charter This sets out the role and objectives of internal audit and is at the core of the delivery of audit services. This is the starting place for a new audit function. The IIA IPPF covers the audit charter in standard 1000 as follows:

> The purpose, authority, and responsibility of the internal audit activity must be formally defined in an internal audit charter, consistent with the Definition of Internal Auditing, the Code of Ethics, and the Standards. The chief audit executive must periodically review the internal audit charter and present it to senior management and the board for approval.
>
> **Interpretation:** The internal audit charter is a formal document that defines the internal audit activity's purpose, authority, and responsibility. The internal audit charter establishes the internal audit activity's position within the organization; authorizes access to records, personnel, and physical properties relevant to the performance of engagements; and defines the scope of internal audit activities. Final approval of the internal audit charter resides with the board.
> - The nature of assurance services provided to the organization must be defined in the internal audit charter. If assurances are to be provided to parties outside the organization, the nature of these assurances must also be defined in the internal audit charter.
> - The nature of consulting services must be defined in the internal audit charter.
> - Recognition of the Definition of Internal Auditing, the Code of Ethics, and the Standards in the Internal Audit Charter.
> - The mandatory nature of the Definition of Internal Auditing, the Code of Ethics, and the Standards must be recognized in the internal audit charter. The chief audit executive should discuss the Definition of Internal Auditing, the Code of Ethics, and the Standards with senior management and the board.

Apart from basic material included in this supplement, there are also other issues with a fundamental effect on the direction of the new audit service as to whether:

1. Internal audit reports to the organization (the audit committee) or the management (say the chief executive).
2. Internal audit reports on the organization (i.e. issues a formal annual audit report) or reports the results of individual audits.
3. Internal audit will act as a consultancy-based service directed by managers who finance the function and request specific reviews.
4. There are any restrictions on audit access.
5. Audit powers are permanent and provided through the highest decision-making forum in the organization.

The charter represents the hopes and aspirations of the internal audit function and it is important that it is designed to support the delivery of professional audit services. If there are problems at this stage, it is unlikely that a successful audit function will develop in the future.

2. Audit standards The CAE has to decide on two types of standards before the new audit function can be developed – professional and operational standards. The former may be based on those provided by a professional auditing body. It is inappropriate to adopt professional

standards if staff are unable to pass the qualifying examinations and become members of this professional body. By definition one could not guarantee that these standards could be achieved (when using unqualified auditors). Operational standards are more readily achievable since they represent a local interpretation of the professional base. These will have to be agreed upon by the CAE as they will set the tone for audit work. This impacts on recruitment as high standards mean that experienced and capable staff will have to be appointed if they are to comply with, and build on, these standards.

3. The code of conduct Another consideration when setting up a new audit service is whether to set standards of conduct before recruiting staff. This is an ideal opportunity where people join only if they feel they can meet the high standards. Once in post it is difficult to impose new requirements. We would look for all the attributes of honesty, integrity, commitment, loyalty and confidentiality. This enables us to test these factors (wherever possible) when recruiting staff. We could check for criminal records and make detailed enquiries when seeking personal references. We may build in a dress code and special rules on behaviour (say smoking or alcohol consumption).

4. Recruitment and selection It is essential that the 'rounded person' is acquired with a whole package of attributes. Training can only go so far, and we are not talking only about formal qualifications and experience. People who can team build, who communicate well and have a sincere belief in their work are real assets. Those who can develop junior staff and get on well with their colleagues make the role of the CAE more bearable. Reliable individuals who do not gossip or try to 'beat the system' should be sought. Suitable recruitment policies and procedures are essential, although where there is scope to head-hunt, this may be considered. Personal recommendations are another way of getting the right staff, although we must at all times fall in line with organizational policies. We must make sure that we can get rid of staff who are unable to pass their auditing examinations.

5. Training A training budget is essential for the newly formed internal audit unit. This covers the types of training that will be undertaken by both senior and junior staff. We must not make the mistake of assuming that experience can simply be bought in. These people may not be available and it is at times better to employ people who are not yet set in the way they perform audit work. A good mix of experienced and less experienced auditors will provide the best cost/service profile that a competitive audit service must strive to achieve. As a final point, bearing in mind that training is dealt with elsewhere in the handbook, do not resource training as a one-off effort. It must consist of an ongoing programme that evolves as the needs of the audit function change over time.

6. The business risk assessment This is an important part of the development of a new audit function. The general risk survey represents the justification for the new service in that it defines those areas that should be subject to audit coverage. It consists of the ongoing analysis of control needs of the organization with a view to assigning audit resources. The survey directs resources in the right way and should be carried out early on in the process of establishing internal audit. It may not be possible to perform a feasibility study on the need for introducing internal audit without first carrying out this exercise. As long as it is done before significant resources have been acquired, this will probably be acceptable. This is why it is good practice to recruit a good CAE in advance of resourcing the new unit, so that this background work may be completed before we commit any resources.

7. Information systems (IS) audit One issue that should be high on the agenda for the CAE when designing the new internal audit service relates to IS audit. There are several approaches:

1. Create a specialist unit of, say, two (or three) IS auditors.
2. Employ computer auditors and locate them throughout internal audit.
3. Employ an IT 'guru' who is available to help and assist audit staff.
4. Assimilate IS audit expertise throughout the internal audit unit by ensuring that all auditors have a good appreciation of IS and related skills and techniques.
5. Rely on the organization's IS department to provide back-up and support.

IS audit expertise may be acquired at recruitment stage (at premium rates), seconded in or developed on an incremental basis by training and development. There are pros and cons for each approach. IS audit is about performing audits of information systems while also providing an input into internal audit's own IS strategy. Extensive reliance on the organization's IS department promotes good working relationships but at the same time impairs our ability to audit this department. It means that information may not be secured independently by internal audit, but obtained third-hand by IT or operational staff. Many of these arguments apply equally to the provision of a contract audit service. The CAE must be wary of creating an elite section within internal audit that are paid more for IS skills which may become potentially uncontrollable. One useful technique that can be used where auditors do not possess the required IS skills is to second a member of the computing department into internal audit to provide back-up and support. If this secondment works out, we would seek to develop basic auditing skills and make the secondment permanent. The CAE must publish and implement an IS strategy that covers the information needs of internal audit over the next few years.

8. Fraud work There is a need to define a clear policy on the detection and investigation of fraud and irregularities. The CAE would have to draft a policy document that deals with a number of related issues:

- Management's responsibilities to investigate frauds and ensure that they are fully resolved.
- The internal audit role in supporting management.
- Management's responsibilities to establish suitable controls that guard against fraud and irregularity. There is a distinct need for controls that isolate instances where frauds occurred.
- The internal audit role in supporting management.
- Management's responsibilities to take positive action where it has reason to believe that a fraud has occurred.
- The internal audit role in supporting management.
- Key contacts in the organization who deal with police and high-level reports on material fraud.

The CAE should take the initiative in helping to set standards. Clarifying who does what forces the organization to address responsibilities and procedures.

9. Business planning The new CAE should devise and publish a business plan that covers the internal audit unit. This will direct the internal audit function over the next few years and show how resources will be applied to:

- defined organizational control issues
- outline allocation of audit resources

- human resource development plan
- information systems strategy
- a marketing strategy.

This activity is a key role undertaken by the CAE, and should consume much of his/her working hours. Structuring has also been dealt with elsewhere.

10. Assurance and consulting services One question to be tackled early on in the life of the newly formed unit is related to the type of services that will be provided by internal audit. It is incumbent upon the CAE to decide the best way to discharge the audit role and which services will be provided and to which degree. It is possible to break down the audit role into two:

1. Risk-based assurance-based audit of all services: financial, operational, strategic and automated systems.
2. Consultancy projects requested by management into regularity, compliance, VFM, management development and others.

There is a knock-on effect on the adopted strategy, structure and approach to audit work.

11. Budgets While the CAE must seek to negotiate an adequate budget, there is little scope to secure extensive funding at the outset. As the internal audit service is developed and grows, we would expect the budget to receive greater support from the organization and so promote a clear growth. This is not to say that we would wish to secure as much funding as possible, since the more expensive the unit, the greater the recharge and cost to clients. Going back to an earlier point where internal audit was broken down into audit services and consultancy services, we can protect the budget for audit services by making the audit committee the client. Consultancy services may be directly recharged (on a project basis) to management. It goes without saying that the CAE should exercise good budgetary control in spending decisions and keeping a balanced account.

12. The launch of the new service The new service must be introduced to the organization using all the well-known launch techniques. A good way to do this is to undertake presentations to senior management and the audit committee as well as preparing the all-important audit brochure and web-based facility.

13. The audit manual We have kept the audit manual as the last topic to be dealt with when setting up a new internal audit department. The extreme view of the audit manual is that of a process that forces audit management to document its objectives, policies and procedures in a formal and publicized fashion. Most of the matters mentioned above will be documented in a section of the audit manual and there is nothing wrong with allowing this document to grow as the audit unit develops. There are parts of the manual that may be written before the service is established. The CAE may have several months to define what is expected from internal audit and how the services should be delivered before staff are brought in. The manual will change and adapt as the new audit function materializes.

The Internal-Audit Function, From Step Zero

By Dan Swanson, *Compliance Week Columnist*

Internal auditing can provide managers and the board with valuable assistance by giving objective assurance about their organization's governance, risk-management

and control processes. Establishing a robust internal-audit function is a long-term and worthwhile investment for most organizations because an internal-audit department can act as an independent advisor for the board and senior management. Where an organization has not staffed an internal-audit department the identification of the benefits and role(s) internal audit could play is the initial step. Where an internal-audit function has been in operation, a review of its recent performance to identify improvement opportunities is recommended.

An Executive Sponsor Is Critical

The organization will need an executive sponsor to lead the analysis of the many issues, benefits, costs, activities, and so forth, that are involved in establishing a new internal-audit function. A senior executive from within the organization should drive the research and ''business case'' efforts with engaged oversight and support being provided by the audit committee. You also could consider working with a recruiting company that has done this before, such as by working with them to developing the job specification for the chief audit executive based on what they identify as best practice – although I believe internal ownership of the effort is absolutely vital, and you should not outsource efforts to set up the department because its too important a task. The first important area to explore is what the role and mandate of the internal-audit department should be, that is, what services it should provide and what priorities the function should have. The internal-audit charter should support the audit committee's responsibilities, and the long-term internal-audit plan should present the assurance plans for the internal-audit function and the audit committee.

The assurance requirements of the board and management will be key drivers for determining internal-audit priorities. The chair of the audit committee, the chief executive officer, and the chief financial officer will be the three key executives to be interviewed, although other officers certainly should provide ideas and input. What type of skills will the internal-audit function require? Certainly the obvious audit skills will be needed: audit management, project management, and strong communication skills. Many others are necessary as well. If technology is integral to the long-term success of the organization, then perhaps a strong weighting should be given to IT savvy auditors. If product development is core, then perhaps operationally strong auditors should make up a large part of the internal-audit staff complement. A strong knowledge of current and emerging management practices will be absolutely critical for all organizations. Finally, you'll also need to look at the soft skills including good leadership, effective teamwork, and, above all, good people-management skills.

Internal Audit Should Be Internal To The Organization

There are also many options when resourcing the internal-audit function, from staffing internally to co-sourcing (blending internal and external resourcing), to starting with an outsourced service while various start-up issues get resolved. Personally, I believe a core internally staffed internal-audit function is the best route, with use of selective outsourced or internal subject-matter experts to augment the core group's efforts. Also, during the first few years in particular, the assistance of audit consultants with different backgrounds and expertise can provide valuable contributions to the

successful launch of the new audit function. As internal audit is often viewed as an integral part of training for high potential employees, the organizational design should provide for two-year or other rotational positions.

Audit best practices are important to every internal-audit function. Operating below acceptable standards is never acceptable and learning from others' efforts is always strongly recommended. There are a variety of benchmarking services available, as well as leading edge information from professional associations and various audit-service providers and vendors that may be helpful. For an existing internal-audit function, an external quality-assessment review can provide many helpful suggestions. It is also important that you implement an objective and independent audit function and a solid reporting line to the audit committee – a dotted reporting line to the CEO will help meet this need.

Investment In Tools, Techniques, & Technology Recommended

The internal-audit processes are another important area that must be explored. For example:

- Do you want electronic working paper files?
- What technology requirements will the new function need?

People are your most important resource and, with the internal-audit function, this notion is no different. Staffing the function, particularly the CAE position, needs to be handled professionally and with an eye towards the long-term requirements of the organization.

The Institute of Internal Auditors has developed a variety of papers and other guidance including a comprehensive 16-step ''roadmap'' repository (for establishing the internal-audit function) that includes links to various resources to assist your efforts. The board, audit committee, and executive management must be satisfied that the new internal-audit function they implement will be appropriate and add value to the organization. A robust internal-audit function strengthens corporate performance and provides assurance to the audit committee and the board that the organization is doing all the things it should be doing. Finally, for organizations that have a few internal auditors on staff – i.e., they have a ''token'' internal-audit function – perhaps its time to consider whether the organization should establish an effective internal-audit function that truly can add value to the organization.

Reprinted from *Compliance Week*. This article was originally published in Compliance Week. Reproduced by permission of Compliance Week. All rights reserved.

8.9 The Outsourcing Approach

The internal audit strategy tells the organization what it will get from its in-house audit team. Progressive management knows what it can get from its audit shop and has very demanding expectations. Where the in-house team cannot meet these expectations without help from

outsiders, then the question of outsourcing arises. The IIA recognizes that internal auditing may be provided through a variety of different arrangements.

The IIA has also provided a perspective on outsourcing of the internal audit function, and selected extracts are summarized below:

> Research shows that effective internal auditing departments are interwoven into the fabric of their organizations. The work of these departments is integral to the efforts of management. The effectiveness of internal auditing begins with a vision statement, which is based on and linked to the overall organizational vision, and is implemented through a strategic plan. An internal auditing department with vision is:
>
> - **Proactive:** It establishes itself as a change agent throughout the organization. It identifies new initiatives to add value to the organization while retaining a clear focus on traditional audit areas such as internal control exposure and potential ethical issues.
> - **Innovative:** The innovative internal auditing department searches out the most valuable use of its resources, questions the value of routine audits, and creates opportunities to increase the value of the function. The department invests in technology, people, and the organization and partners with an external provider if it enhances the value of its services.
> - **Focused:** Auditing must be responsive to the organization it serves. It must understand and focus on management and audit committee priorities.
> - **Motivated:** A motivated auditing staff has a sense of mission, teamwork, and organizational pride. They are open to constructive suggestions and seek input on continuous improvement. They measure user satisfaction and are not resistant to change.
> - **Integrated:** Technology should be used to enhance audit productivity and teamwork. Investments should be made in technology that will assist the organization in continuous monitoring of transactions and identifying potential fraudulent transactions.
>
> **The Future:** Many of the above attributes are obtained with a strong department housed within the organization. External providers may also rank highly on all of these attributes. It is up to management, the audit committee, and the board to assess the various factors and choose the right vision for their organization.[14]

There is also an IIA Practice Advisory (1210.A1-1) that covers obtaining external service providers to support or complement the internal audit activity that contains a great deal of guidance, extracts of which follow:

> Each member of the internal audit activity need not be qualified in all disciplines. The internal audit activity may use external service providers or internal resources that are qualified in disciplines such as accounting, auditing, economics, finance, statistics, information technology, engineering, taxation, law, environmental affairs, and other areas as needed to meet the internal audit activity's responsibilities.
>
> 1. An external service provider is a person or firm, independent of the organization, who has special knowledge, skill, and experience in a particular discipline. External service providers include actuaries, accountants, appraisers, culture or language experts, environmental specialists, fraud investigators, lawyers, engineers, geologists, security specialists, statisticians, information technology specialists, the organization's external auditors, and other audit organizations. An external service provider may be engaged by the board, senior management, or the chief audit executive (CAE).

1. External service providers may be used by the internal audit activity in connection with, among other things:
   - Achievement of the objectives in the engagement work schedule.
   - Audit activities where a specialized skill and knowledge are needed such as information technology, statistics, taxes, or language translations.
   - Valuations of assets such as land and buildings, works of art, precious gems, investments, and complex financial instruments.
   - Determination of quantities or physical condition of certain assets such as mineral and petroleum reserves.
   - Measuring the work completed and to be completed on contracts in progress.
   - Fraud and security investigations.
   - Determination of amounts, by using specialized methods such as actuarial determinations of employee benefit obligations.
   - Interpretation of legal, technical, and regulatory requirements.
   - Evaluation of the internal audit activity's quality assurance and improvement program in conformance with the Standards.
   - Mergers and acquisitions.
   - Consulting on risk management and other matters.

The challenge has been set. Standards have been published that are miles away from the sleepy image of past day audit teams that churned out reams of mindless reports that were ignored or just tolerated. While this drive has lifted the audit profile immensely, it has also raised the bar and created a potential stumbling block for those who have not positioned themselves properly. Out-sourcing, co-sourcing and partnering are always options either as part of the internal audit strategy or because of failure of the strategy to make a mark. The CAE should ensure work complies with the IIA Standards: the use of the provider may be referred to in the engagement communication.

Some internal audit shops are turning towards a partnering arrangement, where they use parts of an external firm's expertise to fill in the gaps between strategic requirements and current capacity. This 'co-sourcing' model has various positives as well as various negatives that have been well described by Paul J. Smith Jr:

> The advantages of using a cosourcing arrangement are numerous:
>
> - Service partners frequently have skills that are not feasible to develop in-house.
> - Outsiders can add a fresh perspective to internal auditing's processes; they often see improvement opportunities not seen by insiders. They may have better, faster, and cheaper ways to perform audits, or see reasons to stop performing them. For example, an external firm showed us we were simply 'checking the checker' in many gas contract compliance audits and were adding little value to the organization. Accordingly, we reduced the number of contracts audited and improved our focus on the ones we continued to audit.
> - Pairing in-house auditors with service partners can broaden the auditors' knowledge and skills, which can be an important career development step for them.
> - Service partners can help cover staff contingencies, such as meeting a client's request for an unexpected audit. A long-standing relationship with a local practitioner has helped us realize this advantage on numerous occasions.
> - Service partners are easier to remove than employees. On one occasion, we employed a service partner to perform an IT audit and it quickly became apparent that the partner's auditor was a bad fit. A phone call was all it took to get a replacement.

Cosourcing comes with its own set of disadvantages, as well.

- You can never be sure what you are getting with first-time service partners. They may not work out, and you will have to replace them. Although it is easier to replace a contractor, it nevertheless means you have to start over, which can be time consuming, costly, and painful.
- Corporate cultures are unique, with their own visions, values, and ways of communicating. This can be problematic for new service partners and can lead to missteps. Repeat service partners can help defuse this problem, but acculturation challenges are inevitable.
- The in-house staff may resent the assignment of a service partner to a project that they believe they can perform. This may be true especially in the case of a high-profile project where it is not clear why a service partner needs to be engaged to perform it.
- It is easy to get hooked on dependable service partners. It is human nature to stick with what works. On occasion, our clients' willingness to listen more closely to someone from a prestigious firm has helped propel this dependency.

The resources required to plan and implement an effective cosourcing arrangement can be significant. And sometimes the perceived benefits will not be realized for a variety of reasons.[15]

Many internal audit strategies are based on retaining a fully resourced internal audit capacity. The IIA Research Foundation has commissioned research into outsourcing and a report by Larry E. Rittenberg and Mark A. Covaleski identified some of the important themes across the companies that have successfully maintained the in-house internal auditing function, extracts of which include:

1. **Organizational Relationships:**
   - an integral part of the organization – clearly defined mission reinforced by management . . .
   - excellent communication – both informal and formal with top management and auditees . . .
   - strong audit committee relationships – regular meetings without management present . . .
   - open to new ideas – eg CSA . . .
   - importance of performance evaluations – interested in adding value . . .
   - training ground for the organization – side benefit of committed internal auditors spread through the organization . . .
2. **Audit Process and Philosophy:**
   - use of technology as an integral part of the audit function – unique perspective of data to help analyse problems across organizational functions . . .
   - an integrated risk analysis approach – understood broad concepts of organizational risk . . .
   - flexible audit plans – reserved time for 'need now' assignments . . .
   - operational/service orientation – willing to service of task forces without assuming responsibility for the solution . . .
3. **Individual Qualities:**
   - experienced personnel who understand the organization – all of the auditors were 'grounded' in some aspect of company operations . . .
   - downsized – 'lean and mean' . . .
   - commitment to staff development – seen as a serious issue . . .
   - will call upon outside assistance when appropriate – either from within the organization or externally.[16]

Andy Wynne on Outsourcing

Andy has provided an interesting discussion for the Handbook on the issues and considerations that result from the outsourcing question and the text of this paper follows:

Outsourcing Internal Audit – a high-risk option? Outsourcing continues to be considered as an attractive option for many organizations. The argument is that outsourcing non-core activities allows a company to concentrate its energies and management expertise on those activities in which it has a competitive advantage. In the public sector, the best value regime in local government for example, requires all services to be subject to the four Cs, one of which is competition.

With internal auditing in particular there are a range of accountancy firms and other organizations who are prepared to provide internal audit and other services. For this reason, internal audit is often considered to be a suitable candidate for outsourcing. In a similarly vein, the Sharman report on accountability and audit in central government argued that the National Audit Office should increase the proportion of its work that is outsourced from 17% to 25%. However, as this article will attempt to show, there are a number of significant risks that any organization should consider before outsourcing its internal audit function.

If a function is to be outsourced it is important that the management of this process can be undertaken in such a way that high quality services are obtained at a reasonable cost with the minimum of effort. The function should be clearly specified, its outputs unambiguously defined and it should be simple to monitor the quality of service that is provided.

The role of internal audit is not clearly defined, therefore it is difficult to specify the function. The revised Institute of Internal Auditors' definition of internal audit states that 'Internal auditing is an independent, objective assurance and consulting activity. . . .' So how is it possible to define the outcome or even output of a consulting or review function?

At its simplest the output of internal audit is a series of recommendations to improve the internal control system under review and an opinion on the quality of that control system. If an internal audit assignment is undertaken and the opinion is that the control system is basically sound and only two or three minor recommendations for improvement are suggested, is this an adequate outcome? It may be that an excellent piece of work has been completed and that significant assurance can be placed on this work. All significant risks to the achievement of the systems objectives may already be competently managed. Alternatively the internal auditors may have only undertaken a superficial review, misunderstood the risks to the system and accepted uncritically the assurances that staff provided them. They may have missed serious weaknesses in the internal control system; failed to robustly test key controls and formed inappropriate opinions on the quality of the control systems. Thus it is very difficult to determine, without replicating the internal audit work, whether its output is satisfactory and the opinion is appropriate.

Most internal audit contracts are defined in terms of inputs rather than outputs. A supplier will contract to provide a certain number of days of internal audit resource and will usually undertake to provide a certain proportion of these with 'qualified staff.' Qualifications do not necessarily provide suitable indicators of quality. The ability to pass examinations (by uncritically regurgitating facts) may not necessarily be an accurate indicator of a person's ability to quickly identify, understand and critically review a complex system. Where qualifications are accepted as a proxy for the quality of internal auditors they are not necessarily checked. For example, in over five years of working for an outsourced internal audit provider I was never once asked to confirm my qualifications.

It is not even easy for an organization to confirm the number of internal auditor days that are provided. Staff may be working on files for other clients when they are present at the organization. Alternatively, they may undertake work for the organization when they are not

on site. However, monitoring the number of audit days provided should be a key aspect of managing an internal audit contract.

The competitive edge of accountancy firms and others supplying internal audit services comes from their ability to use cheaper (usually less experienced and less well qualified) staff to undertake the internal audit work and to do the work in less time. The firm appointed will have a financial incentive to reduce the quality of staff provided to undertake the work and for this to be completed in fewer days than planned. In addition, competition should not be relied upon to ensure that prices are as keen as possible. A recent National Audit Office report on purchasing professional services estimated that government departments could save 10% of the cost of these services by effective procurement practices. Or, putting it another way the government was being overcharged by £60 million a year.

Internal audit providers have even developed a specialist term for undertaking audit work in less days than was budgeted. It is called 'decoupling.' If an audit assignment of 20 days is decoupled it may be completed in only 15 days.

This may indicate greater efficiency on the part of the audit staff. It may even be done in agreement with the client's managers. The director of finance may be happy to pay for 20 days work that is actually done in 15 days if the staff used have significantly more experience or particular expertise. However, decoupling when done without client agreement is fraud. The fact that this has its own specialist term suggests the practice is not uncommon.

Where staff of a similar quality are used, the length of time spent on an internal audit assignment will generally indicate the depth of coverage achieved. The greater the time spent, the greater assurance will be gained that all significant weaknesses within the system have been identified. However, there will be diminishing returns, the amount of time spent on an audit assignment (the cost) should balance the benefits (value of assurance gained and improvements suggested).

The problem is that the point at which this balance is achieved will be different for the internal audit service provider and for the organization itself. An outsourced internal audit provider will generally consider that internal audits should be undertaken quicker with less comprehensive coverage than the interests of the organization would suggest.

This may be demonstrated algebraically. The value to an organization of an internal audit assignment may be expressed by the following equation:

$$V = IR \times ICR$$

where

V	is the value of the assignment
IR	is the value of the inherent risks in the system
ICR	is the risk that existing internal controls will fail to manage the risks

Thus if the value of the inherent risks in a system are £100,000 and there is a 25% risk the internal controls will not prevent the risks crystallizing then the value of the assignment will be:

$$V = £10,000 \times 0.25 = £2,500$$

Thus if an audit costs £250 a day this would suggest a budget of 10 days.

However, from the internal audit service provider's point of view the value of an assignment is reduced by an additional factor that represents the risk of an inappropriate opinion being identified. Thus for the same assignment the value of the assignment will be reduced as follows:

$$V = IR \times ICR \times DR$$

where DR is the risk of an inappropriate opinion being identified.

If *DR* is 80% then:

$$V = £10,000 \times 0.25 \times 0.8 = £2,000$$

This would indicate a budget of only 8 days.

These equations may indicate why outsourced internal audit service providers generally propose internal audit assignments with smaller budgets than in-house staff. It may not be, as is generally supposed, that the audit providers are more efficient. It could be that from their perspective it is just not worth undertaking the audit assignment to the same depth as the in-house staff would consider necessary.

Thus outsourced internal audit providers may propose smaller budgets for internal audit, but this may not be in the interests of the organization. The benefits from further internal audit input may outweigh the costs. This problem is accentuated, as outsourced internal audit is generally more expensive on a daily rate basis.

The higher daily rates are also masked by the reduced budgets of outsourced internal audit. For example an in-house service may cost £250 a day and suggest an annual budget of 1,000 audit days. This would give an annual cost of (£350 × 1000) = £250,000.

If the internal audit service was outsourced the daily rate may increase to £300 a day. However, if the audit providers agree an annual budget of only 800 days the annual cost would be less (£300 × 800 = £240,000).

There are also a number of reasons why an outsourced internal audit service may be less effective than an in-house service even if the outsourced service provides staff of a comparable quality. The core aspect of each internal audit assignment consists of the internal auditor critically reviewing with the system's manager the quality of the internal controls. To be successful this process requires the manager to be put at ease and to be open about any potential problems. This will be less likely to happen if the internal auditor is an outsider who is not considered to understand the organization's problems and the pressures that the managers face.

The outsourced internal auditor may not be able to empathize with the manager. They work for different organizations with different objectives and goals. The outsourced internal auditors may consider themselves to be superior experts brought in to help the less experienced managers. The manager may be more reticent to share problems with a confident outsider who sees any weaknesses in the internal control system as further evidence of their own superiority.

Where the internal audit service is outsourced to a major accountancy firm reliance may be placed on the firm's own quality procedures and its brand image. However, this may not necessarily be justified. In the last five years, according to the Public Accounts Committee, the government has claims against the big five accountancy firms totalling approximately £500 million a year. In addition, several of these firms may not supply dedicated professional internal audit staff and internal audit work may be considered of lower status, something the more experienced staff try to avoid. The FEFC Audit Service found that at least 25% of the internal work at colleges of further education was not of a satisfactory standard. The big five accountancy firms provided much of this work.

As an alternative, organizations may rely on their external auditors to monitor the work of their internal audit service providers. However, this may again not be an effective approach. Internal and external audit staff have different approaches and objectives. They may be fellow professionals, but they come from distinct and separate branches of that profession. Dentists and brain surgeons are both 'head doctors' but you would not rely on one to monitor the work of the other!

There are also ancillary benefits of having an in-house internal audit service. A spell in internal audit can be of tremendous benefit to trainee accountants and other managers. It instils an awareness of the importance of internal controls and a critical attitude that encourages continuous improvement. Internal audit can also be of benefit as an internal consultancy service.

If internal audit is outsourced, this service may change to being used to identify potential consultancy services that can be sold back at premium rates.

It may be considered that outsourcing an internal audit service may enhance its independence. This may not necessarily be the case. Internal audit contracts are often let on a short duration of three years or less. The internal auditors may have only just established themselves and really begun to understand the organization before they start thinking about trying to win the contract again. In this situation they may wish to avoid critical or controversial audit reports that may not be welcomed by senior managers who could have a say on whether the contract is renewed.

Independence should not be confused with ignorance. Internal auditors from outsourced audit shops will almost certainly not fully appreciate the particular culture and ethos of an organization. This is necessary to be effective in identifying sub-optimal control systems and recommending the most effective solutions and improvements. It is difficult for outside internal auditors to be fully tapped into the grapevine of an organization that they only visit from time to time.

For many smaller organizations there may be no realistic alternative to buying in internal audit services from an external supplier. If an organization is large enough to sustain its own reasonably sized internal audit department the in-house service will almost certainly provide a better quality service that is more cost effective than an external supplier. If the internal audit service is outsourced, careful thought should be given to the specification of the service and the way that the quality of the service is to be monitored. Without proper specification, monitoring and management, outsourcing internal audit may be a high-risk option.

A Practical Example

The outsourcing of internal audit represents a threat to many internal audit shops and they survive by being ahead of the game. Where the external auditor also provides the internal audit service, then again this may decrease the overall accountability arrangements and be subject to some criticism. Where the internal audit contract is performed by one of the large accounting firms, it could end up being a series of low-level reviews that are carried out very quickly by junior staff. This arrangement could lead to internal audit returning to the backwaters as a low-level financial checking mechanism. On the other hand, there are some very successful outsourced internal audits that have provided a value-added service and made auditing a leading edge profession. One such contract is now described in outline.

Some years ago a decision was made to outsource the internal audit role on the grounds of cost. The previous in-house arrangements suffered from a combination of the following:

- Highly graded staff.
- Very little planned audits completed.
- Most of the work was reactive in nature and mainly consisted of fraud and other investigations.
- External audit could place little reliance on the internal audit work.
- The total spend on internal audit capacity was around £1.5 million.
- The organization wanted access to specialist expertise to help with the tremendous level of change that it was currently facing.

The new outsourced internal audit arrangements were based around 15 core business systems and the work provided enabled external audit to reduce their fees by some £200,000 pa, while the contract cost less than £250,000. The contracting process started with a request for expressions of interest and the contract specification was not too detailed but indicated the problem and

asked for solutions, based on a three-year contract, renewable for two years. The audit universe was given to the bidders and they were asked how they would cover it through planned audits of financial systems, IS systems, contracts, service delivery and establishments. The in-house CAE maintained a strategic position as the corporate client and client manager. While each of the bidders could have provided the required coverage, the panel was particularly interested in aspects of their presentations that dealt with:

- competence
- capacity
- track record
- cost
- whether they could be trusted to work with as a partner
- how they would translate the given audit budget into outputs.

The panel was interested in the way bidders behaved and how much they listened to the panel members who wanted a tailored service and not an off-the-shelf package. The selected firm proposed a solution that focused on where the organization stood, and, for example, proposed a series of control awareness workshops and other innovative (and people-based) ideas to address flaws in the control environment. The settling down process involved getting the new auditors to meet business managers and many meetings with the contract manager (partner) who would drive the audit work. Key performance indicators were established including customer surveys where the firm was expected to score highly in terms of customer satisfaction. The customer survey results were built into the performance appraisal scheme for the firm's audit staff to reinforce their importance. The firm's own quality assurance system was also examined to make sure it made sense. Early problems were quickly resolved. The CAE worked with the contract partner to get a good understanding of levels of detail and coverage required. The internal audit contract was retendered after several years and this time was offered in three bundles, where firms could bid for one or more, covering:

- planned systems audits
- establishment audits
- fraud work.

Again, the panel looked for firms who had capacity, a client-friendly approach and matched their solutions to where the organization stood in terms of its risk management strategy. There are several hot tips for organizations when going to the market for competitive bid including the following:

- Make a good business case for the contract.
- Be clear about the solution being offered by the firms and how they add value to the organization's strategy.
- Engage with the firms early on when developing a specification that bidders can work with to encourage a good number of bids.
- Select people you can work with, so look at behavioural issues and whether the bidders are convincing and engender mutual respect.
- Do not get boxed in by the legal contract clarifications and measurements. There needs to be a balancing and some sharing of risk on both sides, rather than just relying on contract penalties.
- Do not miss the big picture in contract monitoring – look at outputs, outcomes and pick up real issues.

- Seek to get to co-working in all respects without too many needless demarcations between client and contractor so that the relationship is balanced.
- Ensure all draft reports go to the CAE before sending out to client.
- Establish KPIs for the supplier and make them sensible and workable.
- Place a lot of reliance on post-audit customer questionnaires that go directly to the CAE.
- Focus on outcomes such as the implementation of recommendations and the value add proposition.
- Make sure the coverage is risk based in line with the corporate risk register.
- Think about access to expertise in areas such as HR, performance management, compliance work, control awareness, e-business and security that can be obtained at favourable rates from the provider.
- Find out where CSA fits in and whether this can occur before an audit to focus the audit work.
- Define clear shortlisting criteria covering such considerations as client references, relevant experience, size and structure of firm, technical/professional capacity, professional conduct and so on and give weight to each criteria before each bidder is scored against them (from, say, 0 = poor to 10 = excellent).
- Set values in the contract such as: has the right set of objectives that meet corporate priorities, knows what customers want and need from the service, is provided at best value for money and with maximum impact, adds value to the organization.
- Make reference to meeting the requirements of professional standards such as those issued by the IIA, due professional care requirements and quality assurance models.
- Mention integration of audit process with the organization's performance initiatives, risk management, e-business, anti-fraud measures, ad hoc demand-led work, communicating and consulting with users and regulators and making presentations to the audit committee.
- Make specific demands such as the supplier brings an appropriate mix of skills with continuity and stability of staff working on the contract and brings innovations to the service, e.g. CRSA, audit automation and modern data interrogation.
- Make it clear that all files and working papers are to be handed over and retained permanently by the organization.
- Mention audit approaches (e.g. risk-based systems audits) and criteria for determining testing levels.

Vulnerability

Michael Lapelosa recommends that every six months we take the self-assessment quiz to find out where we stand, covering:

1. How much does your department cost?
2. How much training has your staff received in the past year?
3. How familiar is your staff with the organization's technology and business?
4. How many new, first-year audits have you done in the past 18 months?
5. What percentage of your staff has two certifications?
6. What is your audit cycle time?
7. Have you satisfied your customers?
8. If the internal audit department were your own private business, would you be satisfied with it?
9. How can you make it better?[17]

The Changing Nature of the Audit Shop

An IIA study on outsourcing described the new-look internal audit shop that will be able to address outsourcing as an opportunity rather than as a threat to become smaller, more professionally trained, more experienced, and willing to work with management task forces in solving problems rather than just identifying them. It also concluded that while external audit independence is a potential problem, outsourcing is not the 'make or break' issue.[18]

This challenge has been reinforced by Neil Cowan who argues that:

> Internal auditors are not quasi external auditors. It is a different job that has to be done, utilising many different commonalities. Nonetheless, organisations must specify what it is they want from internal audit and, having specified, they must review performance. The challenge for internal auditors then, whether from the standpoint of inside or outside an organisation, must be to perform up to and beyond expectation. Don't look over your shoulder any more! Look at the service you are providing now. If it's as good as you think it is, you'll be carrying out internal audits for your organisation for a long time to come.[19]

One interesting self-assessment model has been compiled by Steve Wills who asks audit shops to decide which of a series of statements apply to them:

- My internal audit function provides the business with ideas for cost saving and business process improvements.
- The board and senior management view internal audit as a valuable support function and seek internal audit advice before embarking upon new initiatives.
- The board invests in improving the internal audit function.
- My internal audit function provides the business with a full range of assurance expertise.
- The internal audit function has access to technology which enables networked collaborations and facilitates knowledge acquisitions.
- My internal audit function completed 100% of the annual audit plan last year.
- The challenge for the internal audit function is significant – to move from a 'watch dog' to a corporate challenger. From focusing on compliance and financial control matters, to contesting the status quo and monitoring the entire risk portfolio of the business by constantly identifying changes in market conditions, regulations, technology and other industry trends.[20]

Even where the audit shop is fairly small, it may still be retained in-house. The IIA Handbook Series has described strategies for small audit shops against the background of problems including disruption of planned work due to:

- Additional assignments and projects not factored in to the original plan.
- A larger than expected amount of time spent on administrative duties.
- The loss of a team member and subsequent recruitment processes.

and has reinforced the need to assign resources through the medium of risk assessment. David O'Regan, the author of *Strategies for Small Audit Shops*, suggests that the following five traits of internal auditing professionalism may, perhaps, be the most important ones:

1. A credible organizational status with a sound relationship with the organization's audit committee.
2. A well drafted charter defining – among other things – responsibilities, scope of work and a clear commitment to professional standards.

3. A participative approach to the organization's management and employees, which encourages those responsible for specific processes, assets, and liabilities to take responsibility for risk and control in their areas.
4. The use of risk assessment to focus resources and to add value to the organization.
5. A consistently courteous and professional demeanour in all contexts.[21]

8.10 The Audit Planning Process

Planning is fundamental to successful auditing and should involve the client in defining areas for review via the assessment of relative risk. Long-term planning allocates scarce audit resources to the huge audit universe and it is impossible to audit everything. Auditors must be seen to be doing important work. The worst-case scenario is where they are unable to perform sensitive high-level investigations on management's behalf while at the same time appearing to be involved in routine low-level checking in insignificant parts of the organization. A professional audit service tends to rely more on senior auditors tackling serious high-risk issues.

The Planning Process

Overall planning allows the audit to be part of a carefully thought-out system. This ensures that all planned work is of high priority and that audit resources are used in the best possible way. The main steps in the overall planning process are found in Figure 8.34.

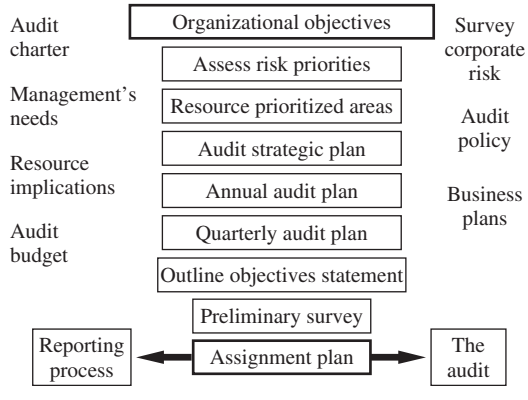


FIGURE 8.34 The planning process.

Some explanations follow:

- **Organizational objectives.** The starting place for audit planning must be in the objectives of the organization. If these objectives are based on devolution of corporate services to business units, then the audit mission must also be so derived. Management must clarify goals and aspirations before plans can be formulated and this feedback can be achieved by active liaison and communication.
- **Assess risk priorities.** The relative risks of each audit area must be identified, with reference to the corporate risk database.

- **Resource-prioritized areas.** Suitable resources for these areas must be provided.
- **Audit strategic plan.** A plan to reconcile workload with existing resources should be developed. This should take on board the various constraints and opportunities that are influential now and in the future. The strategic plan takes us from where we are to where we wish to be over a defined time frame, having due regard for the audit budget.
- **Annual audit plan.** A formal audit plan for the year ahead is expected by most audit committees.
- **Quarterly audit plan.** A quarterly plan can be derived from the annual plan. Most organizations experience constant change making the quarter a suitable time slot for supportive work programmes.
- **Outline objectives statement.** Audit management can make a one-line statement of expectations from an audit from work done so far in the planning process.
- **Preliminary survey.** Background research requires thought on key areas to be covered in an audit. This ranges from a quick look at previous files and a conversation with an operational manager to formal processes of many days of background work involving a full assessment of local business risks.
- **Assignment plan.** We can now draft an assignment plan with formal terms of reference, including budgets, due dates and an audit programme.
- **The audit.** Progress should be monitored with all matters in the terms of reference considered.
- **The reporting process.** Planning feeds naturally into reporting so long as we have made proper reference to our plans throughout the course of the audit.

Audit plans will then flow naturally from the organization's strategic direction while the underlying process should be flexible and, as strategies alter, planned reviews should be reassessed. The flow of planning components should be kept in mind as we consider each aspect of audit planning. The importance of linking plans to objectives can be illustrated:

> A new chief executive joined a large organization and announced far-reaching changes. With several directors dismissed, a different approach to service delivery was evidenced. The audit committee requested a new audit plan in line with a drive to introduce formal risk assessment. The CAE argued it was pointless developing a risk assessment profile until the chief executive had determined the organization's new direction. He argued that audit plans must attach to organizational strategy to be of any use.

The Corporate Risk Assessment

Securing planning information depends on an efficient mechanism to be able to assimilate facts, data and general information into our planning framework. This relies on sophisticated information systems that feed vital material directly into the internal audit risks database. The CAE can be pivotal in setting up such a complex arrangement. The 'risk review' accumulates material relevant to the audit field and assesses impact on predetermined risk criteria. In meetings with senior and line management, the auditor is familiarized with the operation and its key managers. This fact-finding exercise enables data to be obtained and set into audit plans. The features of a corporate risk assessment include the following:

- Meeting with managers is an opportunity not only to get to know them but also to introduce the audit role to clients and gain an appreciation of their concerns. Some of the mystique of audit may be removed. Marketing should be an active feature of client contact and so long as the auditor is competent and presentable, this should create a positive atmosphere. This is a by-product that complements the process of securing relevant material as part of a two-way exchange of information. Information straight from the source saves much time in contrast to straining through reports and decision sheets prepared months ago. Information received from managers is up to date and there is accompanying interpretation and informal remarks that put strategies into perspective.
- It provides material to establish the real risks facing the organization. The risk review provides useful high-level information that provides more than the base operational data and detailed budgets from the audit filing system. Real issues provide real problems, which need real controls. Where audit is able to isolate these concerns, then plans become more dynamic and defensible.
- A useful side effect of the risk review is that link officers may be established in each department/division and provide a vital communication device between the audit field and management. Regular exchange of information assists planning by making it more efficient and responsive. Communication needs to be two-way. The link officers will provide information to audit but will want advice and assistance on new problems with control implications. Providing on-line support to managers diverts resources from planned work. However, there is still a need to resource this type of service in addition to planned audits. We will be expanding on this point later.
- This close contact enables the auditor to follow matters that have been reported previously and get updates on progress in making required improvements to controls. Where a development is inconsistent with a previous audit recommendation, say relating to a live running date for a new computer system, then audit can take up this issue before it is too late. Keeping abreast can enable a form of concurrent audit where a breach of procedure may be spotted before it occurs as the proposed activities are reported in operational plans or committee/board reports.
- The main objective of the review is to provide input to the risk assessment process so that suitable plans may be drafted. What is important to audit should also be so for management, if these plans are to be used to interface audit with the organization. The survey tackles high-risk issues through the constant search for information. As we link with managers the concept of risk will be the cause of much debate and discussion. Once established, the risk criterion may be used to great effect as we sell the idea of risk throughout the organization. Since it is agreed upon with the audit committee, the criterion can only be amended by formal change procedures.
- There is the opportunity to listen to managers, on the basis that 'listening' is a dynamic technique based around interactive communications. The feedback system can be used to supplement the formal complaints system since it can be used to identify problems with individual auditors or clarify matters complained about. Each of these feedback routines depends on communication systems that fall outside the formal audit reporting process.
- The part of the risk review process that involves meeting with management is aided through questionnaires and checklists that shorten the interview process. Providing managers with extensive lists to complete will frustrate the process of communications links. The auditor who sits back and reads from the list of questions is doomed. A checklist may be used to focus on predefined concerns and as an *aide-mémoire* during an interview. The auditor should prepare

such a document and use this for discussions with senior management as part of the risk review that can cover matters such as the corporate risk registers and issues such as materiality, sensitivity, the state of controls and managerial requirements.

- Auditors should be given specific areas in the organization that they will have responsibility for and then be charged with securing information on them. We will not only be concerned with internal information systems, risk registers and reports but also with information that comes from external sources such as press releases and journals. Keeping this information current should be an important staff performance target reported on regularly. Attendance at seminars, meetings, reviews of new legislation and publications is all part of the general survey procedure. This seeks to keep audit up to date with all matters that impact on the assessment of relative risk to controls throughout the organization. This is no simple matter and the drive from the CAE and audit management should be such that it is deemed an important procedure. Audit management may not be aware of items that have been missed by an auditor under this arrangement, so the motivation and interest must be maintained if files are not to fall into disuse. Rotation of assigned areas stimulates and maintains interest as do regular briefing sessions from staff. A key control is to ensure that material gathered is read and interpreted by the auditor before it is entered into the permanent files. It is possible to use a front sheet that forces the auditor to indicate the implications of new information or developments for audit plans. Changes in business risks should be automatically entered into the risk profile and so audit plans should be changed at the regular review dates, say monthly or quarterly. Responsibility for these changes must be placed with the audit staff.
- A filing system can hold the database of information and so smooth the survey data. This records information relating specifically to the adopted risk criteria by providing a suitable document for each key factor. This focuses the survey by turning it from a general information gathering process to a structured method for ensuring key points are addressed. After the completion of each audit assignment, we would remove documents with lasting influence from the current file and place them into the relevant permanent file. A firm picture is built up that 'profiles' each audit area.
- The risk review brings management into the planning process and ensures that audit plans are based on the best up-to-date information. It requires skill and a professional approach so as not to become manipulated by management. It is discussion-led rather than a mathematically generated list of audits.
- While the risk review may be based around meetings with management and reviewing information supplied to internal audit, there must be an element of independence in the way this information is procured and used. We cannot simply rely on material supplied by managers as this can give a distorted view. A level of objectivity should be built into the survey process for it to work as a suitable planning tool. The baseline for planning audit assignments must not be influenced by political in-fighting.

Strategy versus Resources

There are two main models of the long-term planning process where each takes a different starting position to arrive at the list of planned audits. The first starts with the risk-assessed needs of the organization and resources this gap through the application of sufficient audit resources. The second starts with available resources and then assigns them to the defined audit field in the most efficient way. This difference in approach is displayed in Figure 8.35.

Looking at Figure 8.35 a limited version of strategic-led planning occurs where we plan for a full complement of staff by assigning work to posts not filled. An expanded version appears

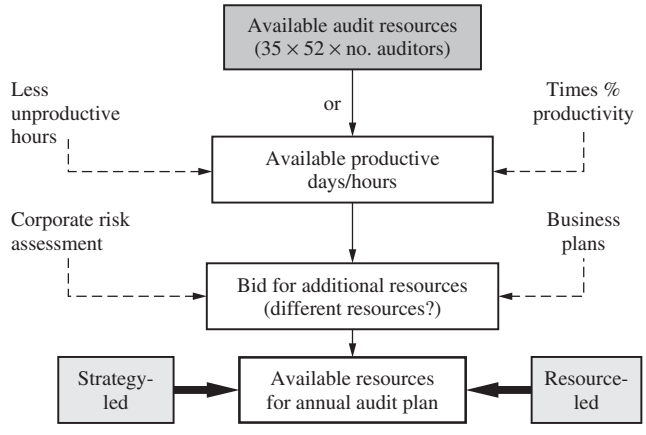


FIGURE 8.35 Strategy versus resource-led planning.

where the required resource level is wholly dependent on the required extent and nature of audit coverage. This assumes full support from the host organization where a new budget will be found to resource the planned audits. In a recession this is hard to defend, although there is increasing use of temporary staff that can fill short-term gaps. The model more often applied is based on planning for the current resources that are available. More often than not there is ongoing pressure to restrict the current staff budget in an annual streamlining process, where it is very difficult to argue that extra resources are required. It is only the newly set up internal audit units that may be able to negotiate an expansion. In a competitive environment, it is not always advisable to seek to increase the staff levels (i.e. budgets) as this may make the audit service more vulnerable as it becomes increasingly expensive.

A Risk Profile

Some audit shops use set criteria to form a risk model for audit planning purposes. For example, four main factors that may be used in a basic model have earlier been defined:

1. materiality
2. impact on reputation (sensitivity)
3. control risk concerns
4. management's concerns.

Each system is appraised on how it scores on these four features, and can be marked from, say, 1 to 10 so that the final score falls between 4 and 40, with the subsequent ranking being in line with the score. The background information for this assessment may be gathered from the general survey.

Each of the four factors is made up of several relevant points:

1. **Materiality**
   - Revenue expenditure.
   - Capital expenditure.
   - Income generated.
   - Level of output.

- Amount of capital invested.
- Space occupied.
- Number of managers and other staff.

2. **Impact on reputation**
   - Political and commercial sensitivity.
   - Type of service provided.
   - Number of sub-systems, inter-linked systems and dependent systems.
   - Importance of objectives.
   - Extent of managerial reliance.
   - Overall affect on the organization's reputation.
3. **Control risk concerns**
   - Past breakdowns in control.
   - Previous frauds.
   - High levels of reported errors.
   - Inherent risks in the operation, e.g. fund transfers involved.
   - Reported evidence of control weaknesses.
   - Recent changes, e.g. new systems.
   - Managerial problems, e.g. long-term vacancies and poor recruitment procedures.
   - Generally lax controls with evidence of non-compliance.
   - Lack of reviews in the past.
   - Previous reviews (and audits) that show continuing control problems.
4. **Management concerns**
   - Risk register status.
   - Direct requests for assistance.
   - Any potential for embarrassment.
   - Specific problem areas.
   - Lack of success that management may have had with previous reviews.

If this information is readily available, it will be possible to build up a risk profile on each major operation. The score in the risk profile will determine the place assumed by the operation in audit plans. Returning to the index factors, each individual operation will be assessed in Table 8.6.

TABLE 8.6 Risk index.

Risk factor	*Score 1–10*
Materiality	
Impact on success criteria (sensitivity)	
Management's concerns	
Control concerns	
Total score	4–40

There are clear advantages in performing this task:

- A suitable filing system is designed to reflect the way the audit field has been isolated. It requires audit management to apply their audit methodology through the way audits are defined. This will involve a combination of IS audits, contract audit, financial systems, operational areas and corporate arrangements.

- It provides a database of audits that can be added to as new developments occur throughout the organization. This is the starting place for the audit mission to set out exactly what the organization looks like in terms of its audit profile. This audit profile should be a mirror image of the organization that moves in parallel with changes that arise over the months/years.
- Audits that are performed can always be set within the context of audits that appear in the audit field. The terms of reference for an audit can be developed with the full knowledge of other distinct areas that are treated separately in terms of audit planning. For example, an audit of IT acquisition standards may bring in the question of overall purchasing arrangements for both IT and purchases generally. Where purchasing is listed as a separate audit, auditors are able to see clearly where their work stops and where a different audit takes over. The listing will confirm that there is much work that needs to be done and only a relatively small amount of resources to do it.

The Annual Audit Plan

Audit will be required to publish an annual audit plan formally approved by the audit committee. This lists planned audits for the year and includes a reconciliation of audit resources to required audit cover. The annual plan may be resource-led and based on available audit staff. Alternatively, it may be strategy-led and include a bid for additional staff/expertise to fulfil the proposed workload. The annual plan is important as it represents the justification for resourcing the internal audit service. Moreover, listed audits must be material to top management's search for commercial success. Auditors will have around 214 days a year available, although it is better to form long-term plans on a week-by-week basis. The annual audit plan will set out which parts of the listed systems will be subject to audit cover over the next 12 months without assigning resources to each audit. It is probably enough simply to state against each planned audit whether it is large, medium or small. As a start these categories may be set as an estimated figure, e.g. four weeks (large), two weeks (medium) and one week (small). Some of the features of the annual audit plan are as follows:

- It contains key audit areas for the next 12 months and explains why they were selected through a suitable preamble. This opening discussion should be a scaled-down version of the audit strategy with comments on the main problems facing the organization now and in the immediate future.
- Following from the above, the annual plan needs to be interfaced with the annual report. The report will talk about the state of risk management and internal control in general across the organization, whereas the plan will explain how these concerns will be dealt with by internal audit.
- The plan itself should be circulated to directors for their consideration and comment before being finalized. It will explain the process of risk assessment and agreed-upon risk criteria. The plan cannot be challenged, although we would expect some degree of consultation with executive management and the basis of risk assessment may be commented on by management who may argue that it does not reflect actual risk because of new or changed information. Management cannot insist on a change to the risk assessment parameter as this can only be enforced by the audit committee, although they can certainly express reservations with the planning process. Once top management has seen the plan, it will be presented to the audit committee to be formally adopted. Changes to the plan should likewise be confirmed at audit committee. The annual plan should be well publicized both to the organization and to individual auditors.

The Quarterly Audit Plan

The quarterly audit plan provides an opportunity to take the planning process to greater detail where the various projects may be scheduled over a 13-week period. The quarterly period has much more meaning to both managers and auditors as a time frame in view of the fast pace of business life. Quarterly plans are no longer short-term matters as it becomes increasingly more difficult to predict what factors may influence the organization as new developments arise. The annual plan sets a background to the quarterly plan. Three months is often an appropriate period within which priorities can be set and work assigned. Within this planning framework, it is possible to:

1. Build in the planned absences of individual auditors so that a good idea of the available resources for the period in question can be obtained. The quarterly period is ideal for this, in that we will have some knowledge of staff movements and training, annual leave and sick leave.
2. Plan audit covers weekly as the basis of a work programme for each individual auditor.
3. Enter projected start and completion dates for each audit that can be in detail (e.g. the exact date) or more realistically the week within which the planned start and finish will fall. It is possible to set this level of detail with a manageable time frame.
4. Allocate projects to auditors. This sets the right resources to the right projects in line with relevant factors. It includes skills, experience, special interests and career development.
5. Reprioritize projects on the annual plan. As quarterly plans are prepared, audits are reassigned on the annual plan as detailed changes are made. The link between the annual and quarterly planning mechanisms must be maintained as each is adjusted in line with changing risks.

Audit Planning – What are our Priorities?

Andy Wynne of the ACCA has provided a perspective on audit planning written for the handbook, which is set out below:

> The internal audit planning process, once a simple matter of ensuring coverage of a handful of financial transaction streams, has, with the extended scope of internal audit, become somewhat of a nightmare. One way of approaching this problem is to recognize that internal auditors have to develop not one, but three sets of audit plans in order to achieve the following three objectives:
>
> 1. cyclical coverage of all significant systems to provide annual assurance to senior management and the board on the adequacy and reliability of internal control;
> 2. ensure that systems of internal control in the most vulnerable areas are working efficiently and are continually optimized;
> 3. additional work on the main financial systems to enable the external auditors to place maximum reliance on internal audit work.
>
> The planning process necessary to provide an annual opinion on the whole internal control system will first need to identify all systems and establishments across the organization that could be subject to an internal audit review. This is an important task as any systems not identified will not be subject to audit, but also, the way the entity's systems are grouped for internal audit purposes may have a significant effect on the efficiency of the overall audit process.

The traditional audit needs assessment models that can then be used to undertake an assessment of the relative significance of each of the systems. The following factors can be used to facilitate this process:

- materiality
- sensitivity and
- vulnerability to error/fraud, etc.

The typical output from this aspect of the planning process will be the assigning of priorities of high, medium and low to each of the systems that have been identified. These priorities can then be used to develop a set of plans, for example:

- High: subject to audit review each year.
- Medium: subject to audit every other year.
- Low: subject to audit once in three years.
- Very low: not subject to audit review.

In recent years, the traditional three- or even five-year strategic internal audit plan has lost favour. The reason being that the pace of change is now thought to be so great that it is not considered worth planning forward over such a long period as priorities for internal audit coverage will inevitably change significantly. One alternative is still to produce a strategic internal audit, but for this to cover the coming year and the last two or three years. This would avoid the problem of planning internal audit assignments to be undertaken several years in the future, but would still ensure that cyclical internal audit coverage of all of the organization's most significant systems would still be achieved. This should ensure that a greater range of systems is subject to periodic review by internal audit rather than just the systems that are considered to require coverage in the coming year.

The output of the corporate risk management process should be a list of the most significant risks that the organization faces. This ranking should be established on the basis of possible impact and the likelihood of these risks actually materializing despite the steps currently being taken to reduce them. Some of these risks will arise because of external conditions, which cannot simply be addressed by improvements to internal controls. However, other significant risks will result from deficiencies within the internal control system. It is these deficiencies, which should be identified as priority areas for action by internal audit. Especially those risks where the residual risks are considered to be especially high.

If the organization does not have a formal risk management process this will make this aspect of audit planning much more difficult to achieve and the introduction of such a process will be an important recommendation.

In the absence of a comprehensive risk register, internal audit can also provide a major service to its organization by developing such a register as a by-product of its planning process. The list of the most significant risks that the organization faces can be developed by considering:

- those systems known to internal audit to be relatively poorly controlled,
- those systems that are of particular concern to senior managers.

The ones that keep senior management awake at night are those areas of the organization that are subjected to significant change. All change is a risky business and has a potentially adverse effect on internal control – including external events that impact on the organization, for example – the potential introduction of the Euro.

The result of either risk-based approach will be a prioritized list of areas for internal audit attention. Those areas assessed as high priority from a risk assessment perspective should be

subject to an internal audit review in the short term. The aim of these reviews will be to improve or optimize the systems of internal control rather than providing assurance on their adequacy.

The risk approach to internal audit planning should not result in a strategic multi-year plan being produced. It will produce a single listing indicating the relative priority for review by internal audit of the most significant risks that the organization faces. A decision will then have to be taken on a cut-off point on this list. The most significant risks (or internal control systems identified as being particularly weak) should be reviewed in the first quarter of the first audit year. The other systems may then be reviewed at a later date. However, as the risk that an organization faces inevitably changes relatively quickly this dimension of audit planning should be reviewed quarterly and probably deserves a fundamental revision each year.

The final aspect of audit planning relates to the reliance that the entity's external auditors should place on the work of internal audit. In many public sector organizations, especially local authorities and NHS bodies, the external auditors expect internal audit to undertake substantial testing on each of the external audit's fundamental systems every year. The Sharman report found that the relationship between central government internal auditors and the NAO 'has not been as close as might have been expected.' It suggested this could be improved and referred to the recent joint NAO/HM Treasury guide to cooperation between internal and external auditors.

For many internal audit sections additional work may be undertaken to allow the external auditors to place maximum reliance on their work. That is extra work over and above the plans developed on the basis of the relative significance of each system and the risks that the organization faces.

The additional work that internal audit undertakes to enable greater reliance by the external auditors should be clearly identified and compared to actual savings in external audit fees. In most organizations it will not be appropriate for internal audit to review each of the major financial systems every year. This can usually only be justified if it is balanced with clear and proportionate savings in external audit fees. In addition, internal auditors need to ensure that this process does not occur at the cost of being able to provide a comprehensive opinion on the organization's internal control system or addressing each of its key risks.

Once these three aspects of internal audit planning have been undertaken the plans will need to be integrated to enable short-term annual or quarterly plans to be produced and the resources that are devoted to each of these should be clearly identified and reported to the audit committee. The relative priority that the audit committee assigns to each aspect of internal audit's work can then be used to determine the relative level of resources that should be devoted to each.

Audit needs assessments involve assigning relative, not absolute needs for audit attention. It is not for internal audit to determine level of assurance that the audit committee (working on behalf of the organization's board) requires on the adequacy and reliability of its internal control system. The audit committee's attitude to risk should guide the level of resources devoted to improving or optimizing the internal control system. However, careful analysing and reporting of the multifaceted nature of proposed audit plans should assist the audit committee members to decide on the total resources that the organization should devote to internal audit.

Resource Problems

Business risk analysis is an ongoing long-term process. It depends on extensive information on operational areas over time. It is important to make a start and write a crude model with rule-of-thumb measures and then build on it. A formal identification of the audit universe is a prerequisite to the risk assessment process. There is a link into the audit filing system as

information is assimilated into the files and then into the risk index. This transition should be smooth and is assisted by suitable documentation that can be used to capture data as it is published or obtained. There is no short cut to the time-consuming task of collecting the database and feeding the information into the risk index. Once established, it is simple to update, maintain and develop. Risk is central to audit and allows auditors to decide how time should be applied to a vast audit field. Simple risk indexes, understood and agreed upon by the client, provide a consistent way of assigning risk. This not only helps ensure the efficient use of audit resources but can be used to defend how audits are selected and undertaken. By viewing risk as impacting all aspects of an audit, the work may be carried out to the highest standard with important areas given greater attention. Larry Hubbard has developed several audit planning tips:

- Ask management to co-sign the audit plan.
- Focus on management objectives.
- Explore the viability of facilitating a workshop during the audit planning process to gather information and identify risks and controls.
- Understand the macro-level risk assessment process well enough to know why the current audit is being performed.
- Co-ordinate your audit efforts with the work of other review groups . . .
- Remember that you can't spend the whole audit budget on planning the audit.
- Speed is of the essence in today's business world, and the time required to perform audits is a consideration for all our departments. However, failing to devote enough time to planning can result in audits that are flawed and of little value or relevance. As auditors, we really are there to help; and if we are to provide the information and support that our clients need, we must be sure that we don't give short shrift to one of the most important aspects of our work.[22]

Scoping Out an Audit of Privacy Programs

By Dan Swanson, *Compliance Week Columnist*

Any corporation of any size today must worry about privacy and information security. Protecting sensitive information has always made good sense, but most developed nations now have laws that restrict some uses of at least some types of data. European countries have regulated personal data protection since the mid-1990s. Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) has been on the books since 2001. Asian and Latin America countries have also passed privacy laws. While the U.S. has not implemented a national privacy law, 44 states have their own such laws on the books. The consequences for infractions can be draconian. In short, ensuring that sensitive information is secure is one of the most important jobs internal auditors have.

Information Security Supports Privacy

Put simply, privacy is the confidential preservation of personal and proprietary information that shouldn't be available without the data subject's explicit permission or entitlement. Although companies often limit privacy practices to customer data, the same protection principles can – and usually should – also apply to other kinds of sensitive information, such as employee and business-partner information, proprietary business data, intellectual property, and many other types of information. Since

sensitive data crops up in virtually every corporate function a business has, companies need to take a deep, critical look at the many business needs and legal requirements that affect the ways they collect, use, transmit, and store various types of information. The fundamental restrictions on consumer-oriented information can usually be considered a good ''baseline control'' for all the other privacy and security considerations a company has. That said, a company's specific policies and procedures for data breach notifications, collection limitations, consumer control over data, and other controls will depend on the industry, business practices, customer expectations, and other factors. To respond to the increasing number and level of threats, companies must provide concrete assurance of strategic and comprehensive privacy programs that incorporate managerial, operational, and technical controls. What many think of as information protection – primarily technical controls such as account access management, encryption, and secure software development protocols, and anti-virus software - is just one piece of this complex puzzle. Organizations also need to implement and regularly assess other, generally non-technical controls.

Getting Started on an Audit

Although companies often conceptually and procedurally segregate privacy and information security, the practices are two sides of the same coin and neither can be effectively evaluated in a vacuum. Privacy objectives and obligations provide direction, scope, relevance, and priority for information security controls. Information security provides the confidentiality, availability, and integrity of sensitive information that underpins privacy assurance.

What Auditors Want To See

- Sound, proactive managerial practices, including planning, direction, frequent operational monitoring, and regular reporting.
- A good balance between strategic and tactical goals for both control objectives and operational results.
- Decisions and actions based on facts, not assumptions or habits.
- Well-documented policies, standards, and procedures.
- Documented roles, responsibilities, accountability, and command chains; workforce development; assurance that staff cuts and that absences will not compromise controls; and policies for secure staff turnover.
- Staff awareness, training, and professional development.
- Consistent compliance with policy and procedures by both staff and managers.
- Functional, reliable technical controls.
- Management and staff can recognize and respond to emerging threats and changing risk factors.

Accordingly, privacy audits tend to focus on organizational processes: how information is used; whether those uses are legal, ethical, and supportable from the perspective of the company's relationship with its customers; and how the organization communicates with customers and other entities about its privacy practices.

Information security assessments also evaluate managerial oversight and operational practices, but they tend to be more technically intensive than privacy audits. Auditors look at automated processes for user authentication, systems access, technology configuration, and other security measures within information systems; and management must support this evaluation with functional tests, evidence of system performance, and technical documentation. A typical privacy audit scope includes an evaluation of policies, standards, procedures, and plans for data protection; incident response, and customer consent management; roles, responsibilities, and accountability related to privacy and data protection; data collection and use in relation to intended purposes, legal constraints, and customer consent; employee awareness and education programs as well as employee hiring, transfer, and termination controls; control monitoring and reporting; and existing practices benchmarked against good practices for information security. Privacy and security audits should generally be performed annually, and sometimes more frequently. Within the scope mentioned above, auditors will generally evaluate controls under three major groupings.

Auditing **management controls** encompass the managerial programs, support, and foundations for effective, efficient privacy and data protection programs. In general, management control audits assess whether: privacy and security policies and procedures have been implemented, performance metrics are documented and performance is measured, controls are supported by adequate budgets, staff, and other resources, and a continuous improvement program is in place and operates effectively. Has the organization required personnel to confirm their understanding of privacy policies and procedures before authorizing access to sensitive information?

Auditing **operational controls** encompass operational processes in which privacy and data protection are a factor, how the organization oversees privacy and data protection, and the measurement and improvement of control effectiveness. In general operational control audits assess whether: rules and requirements exist and are documented; controls operate well; employee and managerial actions are in alignment with regulatory requirements; operational processes support privacy and security objectives; and appropriate managers regularly review key performance reports and operating results. One key question to ask: Does the organization periodically perform a risk analysis to determine the potential material harm that could result from the unauthorized manipulation of information and IT systems that support the operations and assets of the organization? That assessment should include potential impacts on:

- brand value;
- stock value and investor relationships;
- legal liability and regulatory sanctions;
- customer and class-action litigation;
- customer and employee loyalty and trust;
- revenue from customers, business partners, and other relationships;
- the assessment should consider and document a worst-case scenario for the compromise, corruption, or misuse of the entire set of data subject to the assessment.

Audits of **technical controls** encompass systems and automated functions that support privacy and data protection goals. Technical controls address risk inherent

in system design, access, and operation, as well as risks inherent in the business processes facilitated by organizational technologies.

Be Proactive

As in all audits, it cannot be overstressed that managers, not auditors, are responsible for defining and implementing solutions to issues found in the audit. Auditors can help management to understand identified risks, best practices, and common privacy and data protection frameworks. Auditors cannot – and should not attempt to – dictate management's response to known deficiencies. Such an effort would undermine auditor independence and degrade the value of the audit process itself.

Reprinted from *Compliance Week*. This article was originally published in Compliance Week. Reproduced by permission of Compliance Week. All rights reserved.

8.11 New Developments

A useful approach to developing an audit strategy is to use the perspective of key stakeholders to work out how best to meet their needs. Most audit shops are working out how they can best contribute to their organizations and have a strategy for adding value as the pressure grows on all resources. One approach is to identify key stakeholders and ensure their needs are being identified and met. A review of the type of questions that an audit committee may well ask regarding the leadership, work and performance of their internal auditors has been prepared by the IIA:

- How well do I know the head of internal auditing?
- How often do I talk to him or her?
- Do I appoint the head of internal auditing? Does he or she report directly to the audit committee?
- When was the last time I reviewed the internal audit charter Do I know what it says?
- Do I know how the internal audit activity sets its plan?
- Do I review and approve the annual plan?
- How well is the management team implementing actions agreed upon during internal audit work?
- If the chief audit executive (CAE) came to me and expressed concerns based on his or her business judgment, would I listen? How would I act?
- Does the internal audit activity comply with The IIA's Standards?
- Is internal auditing's position in the organisation at a sufficiently high level and sufficiently detached from functional areas to guarantee its independence?
- Do the internal auditors avoid activities that could undermine their objectivity?
- Is the internal audit plan based on the organisation's risk profile?
- How well is the internal audit activity completing its plan this year?
- Does internal auditing have a quality assurance program?
- Does it have a plan to undergo an external quality assessment every five years as required by the Standards?
- What are the results of the most recent quality assessment?
- Is internal auditing sufficiently resourced to provide objective assurance on risk and control?
- How does the CAE respond to probing by the audit committee?[23]

Improving the way the CAE interacts with the board's audit committee should be a firm part of the audit strategy and the results of one survey provide a useful insight into this topic:

> Although chief audit executives (CAEs) see themselves as strong supporters of their audit committees, opportunities exist to strengthen the relationship with the committee as well as to become a stronger link between the audit committee and others in the organization who are focused on risk management efforts. CAEs educate audit committees on relevant risks and risk management strategies as well as providing updates on critical issues and information about the internal environment of the organization. To a lesser extent, CAEs are involved with audit committees on increasingly strategic activities such as defining the scope and design of enterprise risk management (ERM) projects or risk assessments. The most effective CAEs strengthen the link between the audit committee and management by effectively exercising their independence and providing proactive information and analysis on pertinent risk and governance issues. CAEs with deep knowledge, broad skills, and solid experience are in a position to serve the audit committee and management most effectively by bringing solutions to the table and acting as a translator between the committee and management on risk management issues.[24]

The conclusions from this research offer some useful advice for the CAE:

> Today, CAEs interact with audit committees in a variety of ways – both formal and informal. Some CAEs are already actively engaged and feel leveraged by the audit committee. Others might have more work to do to develop the relationship. In either case, there are concrete things every CAE can do to increase the value they are able to add to the organization:
>
> - Understand the wants and needs of the committee.
> - Be the corporate governance expert the committee turns to for advice.
> - Establish strong interactions with audit committee members.
> - Build audit committee relationships based on skills. If the CAE has a low level of
> - experience, he or she should ask for mentoring from audit committee members or tap
> - into networks of other CAEs or consultants to learn from their experiences.
> - Work to eliminate any inefficiency in communication between the CAE and the audit committee.
> - Engage with the committee to design the internal audit department's mission, strategy, and focus.
> - Position him- or herself to be a key force in bringing clarity and aligning the contributions from finance, legal, internal audit, and other management functions.
>
> Be prepared. ERM has been identified by audit committees as well as CFOs as the biggest challenge to be faced in the coming months.[25]

It is one thing to set an audit strategy and quite another to ensure the audit resources it astutely to deliver the goods. The IIA standards are challenging in that they represent an ideal that can be daunting for an audit team that is staffed by low-level juniors, or more senior people who have become stuck in their ways. A good example of a staffing strategy comes from the things that the Financial Services Authority looks for in their audit resource, which includes an all important intellectual capacity:

> Hilary's strategy for staffing her team is to have around half of them coming from within the FSA, with the rest recruited externally for their professional audit skills. She has made a number of recruits – there are 16 staff in the department – but still has vacancies for senior roles to fill. A system of guest auditing – a Hilary innovation – allows staff from other parts of the FSA to spend time working in internal audit. The "guests" get an interesting development opportunity, while the internal auditors benefit from their expertise and get to spread the word about what the function does and procurement. So that is in itself a big challenge, a big intellectual challenge."

> That means the number one requirement for an FSA auditor is "intellectual capacity", says Hilary. Number two is gravitas and oral communication skills. "They are key in this because as soon as we walk into a room and speak to people we have to have credibility, all auditors do." Written communication skills are vital, too. "The FSA puts a high premium on the written word and that applies as much internally as externally. Good writing skills, so that clear persuasive reports can be produced quickly, are very important." However important, these skills are just what Hilary regards as "base camp – what you need to get in the door." What else does she look for? "It is critical that we have people who have good influencing skills, who understand the backdrop to what they're doing, and understand how things have come about in the FSA. They need to be able to position things and add the necessary context. Auditees are always asking for more context."[26]

One way of adding value is to ensure the needs of the audit are understood and met. Hanif Barmer has a view on this:

> We've all seen the surveys of what an audit committee expects of an effective head of internal audit: leadership, technical skills, communication skills ... the list goes on. But nobody ever mentions one attribute – the head of internal audit needs to be a mind reader. He or she often needs to know what the audit committee wants – and to be able to deliver this – without being told what is expected!. How will you know when the relationship is working? This is hard to describe, but you'll know when you get there. Some of the indicators will include: periodic emails and phone calls with the audit committee chair between committee meetings; audit committee members stopping by for a chat when they are at head office, even when there's no audit committee meeting scheduled; the audit committee chair asking to be kept informed when an issue comes up but has not been resolved, rather than asking what's being done about it; a few words of praise for internal audit at an audit committee meeting; the audit committee chair asking for your views on an issue at an audit committee meeting. What you'll find most noticeable, though, will be the fact that you've stopped being so aware of the need to make an effort.[27]

Let us take a closer look at the positive contribution that internal audit should be making:

> Buchanan also expects the head of internal audit to make a positive contribution. "You want someone who is walking into the CEO's office at least once a month and offering a bit of insight," he says. They should be raising concerns, flagging risks that are affecting other companies, "acting as a sounding board for the CEO as well as the CFO – someone who operates at that level." And they must have an action based agenda, looking to get things nailed down and finished. He wants someone who is suggesting things that can be implemented, "and not just agonising over worries that go on and on from meeting to meeting." There should be what he calls a programme for closure: "Who will do what for whom and by when? Then it's full stop, turn the page, next item." Summing it all up, he needs "A valued player to the business people, as opposed to some niggly bugger who's going to ask difficult questions without adding a lot of value."[28]

One key question is, how does internal audit show it is adding value, in boom years and when the economy is in recession? Each and every CAE will want to address this question before it is asked by the audit committee. The value add equation should drive the audit strategy in a way that means a successful internal audit function even where there is an economic downturn. Help is at hand with PWC's fifth study into the state of internal auditing:

> If internal audit is to demonstrate value in the face of declining resources, it must begin with a fresh look at the company's internal audit strategy and a reassessment of its own processes. We believe doing so will not only help gain credibility with organizational peers suffering the same cutbacks, it will also help internal audit preserve its capacity to address strategic, operational, and business risks, as well as today's emerging challenges.
>
> As we anticipated in our forward-looking report Internal Audit 2012,1 internal audit leaders have begun to recognize the need to redefine the function's value proposition and seek to increase its value by learning to operate more efficiently, intelligently, and quickly. Concerns over declining budgets are a reminder that greater efficiencies within internal audit won't come a moment too soon.[29]

We now turn to the important issue of contributing to IT governance in adding value to the business. For a view of ways that internal audit can better contribute, we can turn to the IT profession itself:

> There are numerous benefits of having information technology personnel work closely with internal auditors. For some technology personnel, the entire audit function may have a mysterious and misunderstood role, particularly when working in certain industries. Too often, auditing is viewed as a necessary evil, and therefore, will involve confrontational relationships. In high-performing organizations, there is a mutual respect and trust between the technology teams and the internal and external audit teams. In these situations, technology teams view the auditors as additional consultative resources to ensure appropriate controls are in place and effective. Just as the manufacturing world realized the need for quality control processes, technology departments are finally recognizing that processes and controls to ensure the quality of information technology services must be implemented. When IT processes are well documented and operating reliably, IT audits confirm the positive efforts of IT. Where they are not, IT audits report the gaps and numerous opportunities for improvement. The level of documentation for IT processes should reflect the risks associated with the IT processes. IT audits will provide an independent assessment of the appropriateness of the IT efforts to be efficient, effective, and responsive to the needs of the organization.[30]

Protecting and increasing shareholder value is the key to a successful organization and this may be achieved by using the following advice:

> A correctly aligned approach to risk management focuses on those risks with the greatest opportunity to reduce shareholder value. Given that definition, two factors may be to blame when management is unable to effectively identify and respond to risks that can damage shareholder value: the absence of a correctly aligned approach to risk management coupled with the lack of a sufficient engine to power the company's risk management strategy.
>
> A transformed internal audit function has the potential to become that engine – a potent force of old-fashioned due diligence that could help manage the increasingly sophisticated risk factors today's businesses face.[31]

Most argue that real value comes from transforming a service to fit new contexts. In terms of the internal audit function, a 10-step plan is recommended by PwC for just this task:

1. Identify stakeholder expectations of internal audit; ask what management, the board, and the audit committee value.
2. Gather data to assess current state.
3. Link the company's strategic objectives and shareholder value drivers to internal audit's scope.

4. Consider how previously unaudited areas might be audited, then align auditable risks to the audit plan.
5. Eliminate routine, low-value audits.
6. Based on the updated audit plan, consider transformational ideas to reduce cost.
7. Identify inefficient processes.
8. Develop implementation plans for transformational concepts as well as anticipated process efficiencies.
9. Review updated internal audit plan, along with cost-reduction ideas, with key stakeholders to gain support.
10. Implement (add measurement, feedback, and adjustment processes for continuous improvement).[32]

Having got good resources in place, the next stage is to look at the audit plan and how it can be developed in a way that is both dynamic and flexible:

> During rapid transitions from one economic state to another, traditional audit cycles and frequencies may not serve organisations well. This indicates that assurance needs can (and need to) alter at a similar speed and may require key business risks to be audited more frequently. For example, how often does internal audit look at risk management arrangements – annual reviews may no longer be enough. Additionally, audit plans that run for three to five years may no longer be fit for purpose, where a greater responsiveness demanded by the business ought to result in plans covering shorter time periods, involving smaller audits with a quicker turnaround time. External factors will impact upon an organisation's function and health. Many indicators such as the retail prices index and exchange rates are "lag" indicators showing conditions that have happened. Whilst they are useful, they are probably too late in helping an organisation in being proactive and agile to changes. To identify change, the focus needs to be on lead indicators that show which way the wind is blowing. This is what gives an organisation the ability to be ahead of the game and respond to threats in a downturn and to take advantage of opportunities before its competitors during an upturn. This would also require internal auditors to adapt their internal management arrangements to reflect the principles of agility and responsiveness for the use of resources. For example, identifying key staff with specialist skills that will be required when an organisation's future assurance needs change becomes a key consideration. Many organisations make use of tools such as PeSt (political, economic, social and technological) analysis to gauge environmental conditions and inform the business planning.[33]

One major strategic issue relates to the way audit plans its work over the year. The dynamic approach to this task as suggested by some CAEs is that audit need no longer develop annual plan as such but simply build an indicative quarterly plan that flexes as the fast moving risk profiles change and alter with each major new event. An interesting perspective is given by one well-known audit writer:

> If your average commitment, over the course of the year, for management special requests exceeds 10%, you have a planning failure. When management continuously overrides your audit plan with excessive special requests, they are telling you that your plan is wrong, that you are directing your audit resources to the wrong areas, or at the wrong time, and that they are better at allocating your resources than you are. They may be right. The solution is to engage senior management more extensively in your planning discussions, to listen closely to their concerns and

> to ensure they understand the strategy behind your audit plan and the implications of changing your plans to accommodate special requests. Your audit universe should map very closely to your company's organisation chart, lines of business or process structure. You should be auditing the business that management has created and is responsible for. A logical step in the planning process is to gather any risk assessments prepared by management. If they have prepared risk assessments, your assurance strategy must include an evaluation of that assessment to determine its reliability. The solution is to include the reliability of management risk assessments as one of your audit planning criteria. Management with a track record of reliable, comprehensive risk assessments should receive much less audit coverage. Management who do not perform risk assessments should be featured prominently in your audit plan and in your executive and board reporting.[34]

Paul Boyle has explained the concept of audit value in the following way:

> If governance, risk management and internal control provide the framework for business success, it is one in which high-quality internal auditing plays an important part, says Boyle. "Clearly, when it comes to the management of risk, the internal audit function can make a huge contribution to the board's and audit committee's understanding," he says. "An internal audit function can get to the facts, they can make comparisons objectively between different parts of the company, they can identify corrective actions, and they can follow up to make sure those corrective actions are being taken. It's absolutely central." The FRC – as mentioned – makes a conscious effort to put entrepreneurialism ahead of risk, and internal audit functions should do likewise, Boyle believes. "A potential danger for internal audit, and one to watch out for, is that, almost by instinct, their focus would be on the management of risk and not necessarily on entrepreneurial success," he says.[35]

He has also tackled the vexed issue of audit independence in the context of adding value:

> This isn't the only difficult balancing act that internal audit needs to master, Boyle argues. "Another challenge that internal audit faces is how to strike the appropriate balance between independence from the business units and involvement," he says. "If you're completely independent and don't reach out to the business units then you won't necessarily know enough, learn enough, about what's going on to really find out where the risks are. But if you become too involved in helping the business to be entrepreneurially successful then you might lose your independence, your ability to spot risk, because you end up crossing the line and getting wrapped up in the thrill of the chase."[36]

Summary and Conclusions

Many internal audit shops have moved on from the risk assessment checklists and entered into a dialogue with the board about how the audit resource can be used to the best effect, that is, utilizing the corporate assessment of risks along with auditors' special expertise in risk management, control models and specific control mechanisms (and requests for consulting projects), and the way objective assessments can be used to promote accountability and help managers deliver. The author has developed a basic framework for defining three different approaches to audit strategic planning. This paper is reproduced below.

DYNAMIC AUDIT PLANNING

Introduction

The internal audit world has and will continue to change at a pace that many find uncomfortable. New demands create new challenges for the CAE. Audit planning is one area where we need to respond in a positive and dynamic manner. This paper provides a brief introduction to three alternative ways that we may plan our work in this context.

The Three Approaches

1. TRADITIONAL AUDIT PLANNING

The well known approach to planning audit work involves defining a risk index consisting of appropriate factors (e.g. materiality, impact on reputation, state of control risk and management requests). These are applied to the defined audit universe (all systems within the organization) to produce a risk assessed plan of work for the next three to five years. A summary will look like:

Factor	Score	Weight?
Materiality (how big is the system?)	**1–10**	
Impact on reputation (does it matter?)	**1–10**	
State of control (anything going wrong?)	**1–10**	
Management (have they asked for help?)	**1–10**	
Score for the system	**4–40**	

So high-scoring audits receive early attention although we may look at everything on a cyclical basis over the three years. We may also perform detailed transactions testing of key financial systems through the year.

2. CORPORATE GOVERNANCE-BASED PLANNING

A more advanced method revolves around the corporate governance framework. Here we concentrate audit resources on key areas such as:

- Boardroom arrangements and accountabilities.
- Remunerations committee.
- The role and impact of audit committee.
- The impact of NEDs on the board accountability.
- Factors that encourage financial misreporting.
- Reliability of audit committee and external audit coverage (and independence).
- Control framework in use.
- Reporting on internal controls.
- Risk assessment and risk management arrangements.
- Ethical standards and staff awareness.
- Anti-fraud policies and whistleblowing arrangements.
- Project management (including change programmes).
- Control activities – and performance management.
- Information systems (security and integrity).
- Communications – across and up/down the organization.

- Control assurance reporting – and underlying evidence such as CRSA.
- Control environment – and ethics and tone at the top.
- Compliance teams and routines. Fraud policies and security.
- Accreditation systems such as ISO 9000, EFQM, IiP.
- HR policies such as staff training, competencies, vetting and learning programmes.
- Financial systems and validation routines by financial controller.

In this way the internal auditor seeks to 'quality assure' the governance framework established by the board. It takes a hands-off approach and seeks to review whether the above high-level systems are in place and are working for the year in question to promote good corporate governance.

3. RISK-BASED PLANNING

Here we seek a facilitation risk-based approach where we promote risk assessment and review areas of particular concern. This would involve:

- Corporate board level risk assessment – identify and classify key risks (top ten – risk policy).
- Risk management – assign these risks to responsible managers and ensure they establish a risk management framework (avoid, accept, transfer, insure, contingency plans and/or controls).
- Operational level CRSA programmes – where risks are identified and associated controls reviewed by work groups (for action planning).
- Discussion – talk to management about their risk assessment and key controls that they are dependent on.
- Risk database – prepare a risk database and isolate areas of high risk and controls that are crucial to business success, based on the organization's risk management process in operation.
- Discuss the results with the audit committee and allow corporate and operational risk assessment to drive the annual audit plans for assurance and consulting work.

So we focus on helping the board and management establish good risk management practices and then review the areas of continuing concern (i.e. high residual risk) – or simply review key areas deemed critical to business success. The internal audit plan reflects a combination of the supporting role in helping establish risk management (consulting services) and audits of high risk areas (assurance-based) that have been identified by the board and senior management through their risk register.

Conclusions

We have a number of options for planning audit work within the context of corporate governance and risk management. The main guidance suggests that each organization will adopt its own solution that takes on board its risk appetite, environment and organizational culture. Audit will respond accordingly and a planning framework that represents a hybrid of the above three approaches may result (with varying emphasis). Whatever format is adopted the CAE of the future must ensure:

- It fits with the way the organization responds to corporate governance.
- It is mainly driven by the corporate risk register.
- The board/audit committee accepts that this is the best way to apply audit resources.
- It underpins and links into the annual opinion that the CAE provides on the system of internal control.
- It is dynamic, flexible and responds to the changing demands of risk management and accountability.

The CAE is well advised to present a business case for the adopted planning approach (particularly where we move way from a cyclical approach) for approval by the board/audit committee. However, we should remember that whatever one promises to deliver – one must deliver and deliver well. James Roth has considered Seven Roads to Success on behalf of the IIA Research Foundation by posing two questions:

1. Which IA practices add the most value?
2. How can IA identify the practices that will add the most value to their own department's stakeholders?

The research involved interviews with some 20 thought leaders, surveys of 4,600 audit directors/managers (673 responses) and five case studies of specific audit departments. The major changes in internal auditing were described as moving:

1. from confrontational to partnering with management;
2. from detection to prevention;
3. from control or compliance based to risk based;
4. to consulting;
5. from past to future focus;
6. focus on organization's objectives, strategies and risk;
7. to adding value;
8. staffing with internal transfers;
9. focus on contextual areas;
10. technology and e-commerce;
11. knowledge sharing, soft control, CSA, returning responsibility for controls to management.[37]

Chapter 8: Assignment Questions

Having worked through the chapter, the following questions may be attempted (see Appendix A). Note that the question number relates to the section of the chapter that contains the relevant material.

1. Explain the importance of a carefully considered risk-based strategy for the internal auditing service and describe ways that this strategy may be developed and applied.
2. Describe the way in which suitable audit staff may be secured and applied to delivering the set audit strategy.
3. Discuss the pros and cons of formal appraisal schemes for internal audit staff and describe various ways that can be used to measure the performance of individual staff and the audit service in general.
4. Outline the types of problems that may interfere with the performance of the internal audit service and consider ways in which some of these problems may be addressed.
5. Explain why it is important to have an up-to-date audit manual and describe some of the items that may be addressed by the manual.
6. Describe the way action points from the audit strategy may be delegated and explain the measures that may be taken to ensure such delegation is properly controlled.
7. Describe how information systems may be employed to support the audit strategy and explain how audit staff time may be managed through effective information and reporting systems.

8. List the steps that may be taken to get a new internal audit shop up and running and discuss the issues that need to be considered when developing the new audit service for an organization.
9. Describe the steps that may be taken to ensure that internal audit services provided by an outside supplier are efficient, effective and provide added value to the organization.
10. Prepare a presentation to the internal audit management team on the measures that can be taken to arrive at the annual audit plan, which includes a view on the importance of taking on board corporate and business risk assessments (which have been carried out by the board and senior management).

Chapter 8: Multi-choice Questions

8.1 Insert the missing word/s:
Any audit objective must be linked directly into the organization's own objectives (or mission). The starting place for setting audit's role is to isolate what the ..... is trying to achieve and then see how audit resources can assist this.
a. director of finance
b. profession
c. organization
d. regulator

8.2 Which statement is least appropriate?
A risk survey necessitates discussion with middle management and involves:
a. A definition of the audit unit.
b. An assessment of the relative risks inherent in each unit.
c. Research into the type of problems units attract.
d. History of disciplinary action in the unit
e. Risk ranking related to resources subsequently assigned via an audit plan.

8.3 Insert the missing words:
A further aspect of audit strategy relates to the need to ..... in the process. There is a temptation to become trapped inside the struggle to preserve audit independence, wherein contact with the outside world is avoided. Our plans and strategies are then based entirely on audit's perception of organizational needs on a 'we know best' basis. What may have been acceptable in the past can no longer be defended when all expenditure (including audit costs) must be justified to front-line managers whose budgets bear the eventual re-charges.
a. involve management
b. retain independence
c. brief audit staff
d. involve the CAE

8.4 Which statement is least appropriate?
Areas that need attention might jeopardize the welfare of audit. It is vital these are identified and dealt with via the strategy. Common problems are:
a. Excessive non-recoverable hours
b. Low staff morale
c. Lack of audit procedures
d. Out-of-date audit manual
e. High staff turnover
f. Poor client relationships

g. Low-level audit work
h. Recommendations ignored
i. Poor quality of work
j. High level of participation of management in audit planning
k. Assignments over-running budget
l. No career development
m. Poor reputation

8.5 Insert the missing words (they apply to both sentences):
We may feel pressured into conceding that long-term planning must establish formal terms of reference for these planned audits. Fortunately, the ..... comes to the rescue since we need not provide detailed plans for each audit over and above the act of selecting those areas that attract a high level of risk. The ..... allows us to take an audit area and carry out some background work with a view to setting formal terms of reference for the ensuing audit.
a. preliminary survey
b. audit plan
c. risk management
d. terms of reference

8.6 Which statement is most appropriate?
a. Strategic development is getting auditors to work together re-actively to drive the audit service forward in the right direction. The need to rally round a clear goal is fundamental to the success of any strategy.
b. Strategic development is getting auditors to work together proactively to drive the audit service forward in the right direction. The need to rally round a clear audit manual is fundamental to the success of any strategy.
c. Strategic development is getting auditors to work together proactively to drive the audit service forward in the right direction. The need to rally round a clear goal is fundamental to the success of any strategy.
d. Strategic development is forcing auditors to work together proactively to drive the audit service forward in the right direction. The need to rally round a clear goal is fundamental to the success of any strategy.

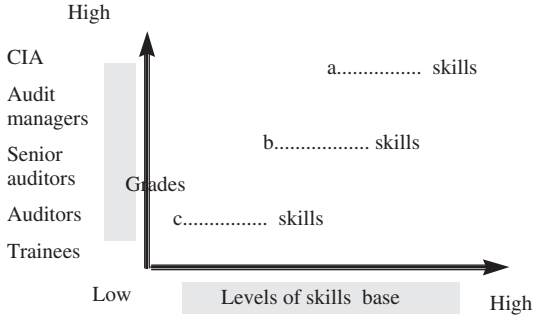
8.7 Which statement is least appropriate?
The next stage in the recruitment procedure is to formally define the requirements of the post. The process of setting the job description is one of considering the ensuing contract of employment that will be entered into by the incoming appointee. This process may be documented as:
a. Define the key responsibilities of the post having regard to other jobs in the section.
b. Include the main components that apply to all audit staff in line with the level of responsibility of the post.
c. Set out the categories of activities that will be required from this job in distinct groups.
d. Write out a formal job description and ensure that it is consistent with the others across the audit department.
e. Carry out a formal job evaluation and assign an appropriate grade to the post that fits with the ability of the person recruited.

8.8 Which statement is most appropriate?
a. The only useful reference is a questionnaire that is sent direct to a colleague of the applicant's current or last employer.

b. The only useful reference is a questionnaire that is sent direct to a named person nominated by the applicant.
c. The only useful reference is a questionnaire that is sent direct to the personnel department of the applicant's current or last employer.
d. The only useful reference is a questionnaire that is given to the applicant to pass onto to his/her current or last employer.

8.9 Which statement is least appropriate?
Whatever the view, it is essential that auditors are appraised in a positive fashion. This in turn depends on:
a. Keeping the accent on praise.
b. Using appraisal to ease poor performers out of contact with clients.
c. Not using the appraisal scheme to criticize but using it to develop.
d. Using performance appraisal to engender good communications and listening skills.
e. Seeking to promote a win–win environment where all sides gain.

8.10 Select the most appropriate description of skills 1, 2 or 3 for levels a, b and c in the diagram.



Types of skills:

1. technical skills
2. writing skills
3. conceptualizing skills
4. listening skills
5. communicating skills

8.11 Which statement is least appropriate?
There are several matters to be considered when designing a performance appraisal scheme, including the following:
a. The scheme must in fact address the auditor's performance.
b. The scheme should attempt to meet employees' needs that should be based around a desire to obtain feedback on their achievements and approach to work.
c. The scheme should represent what can be readily achieved by the auditor.
d. The scheme must incorporate the concept of annual progress reporting.
e. An auditor can compile a career plan so long as there is an awareness of the areas that have been developed and those that need further developing.
f. We can build on this idea of motivation by suggesting that any valid scheme should be geared directly into this concept of releasing 'people power'.
g. The scheme should acknowledge the personal goals of each auditor.
h. The appraisal scheme should ideally feed into a suitable training programme.

i. Performance appraisal should be sophisticated enough to define an auditor's potential to work at a defined level.
j. Using the bridge between performance appraisal and auditor development plans, we can go on to consider the future of each auditor in terms of promoting his/her management skills, existing job and future potential.
k. Counselling is also an important component of an appraisal scheme.

8.12 Which paragraph is most appropriate?

a. The concept of appraising staff must attach to some form of professional foundation for it to have any real meaning. If it is not seen as part of a career development programme, then we return once more to the view that appraisals can have a demotivating effect on the auditor. Appraisals should be founded on a two-sided agreement that seeks to assess the auditor and then help him/her address any identified deficiencies.
b. The concept of appraising staff must attach to some form of professional foundation for it to have any real meaning. If it is not seen as part of a career development programme, then we return once more to the view that appraisals can have a demotivating effect on the auditor. Appraisals should be founded on an agreement that seeks to assess the auditor and isolate any identified deficiencies.
c. The concept of appraising staff must attach to some form of professional foundation for it to have any real meaning. If it is seen as part of a career development programme, then we return once more to the view that appraisals can have a demotivating effect on the auditor. Appraisals should be founded on a two-sided agreement that seeks to assess the auditor and then help him/her address any identified deficiencies.
d. The concept of appraising staff must attach to some form of disciplinary procedure for it to have any real meaning. If it is not seen as part of a career development programme, then we return once more to the view that appraisals can have a demotivating effect on the auditor. Appraisals should be founded on a two-sided agreement that seeks to assess the auditor and then help him/her address any identified deficiencies.

8.13 Which set of performance measures are most appropriate?

For example, a target for a senior auditor may be:

To prepare and implement a new and revised audit manual that complies with best practice and adopted audit standards by date X (using 100 audit hours).

Attached to this would be various performance measures that could form the basis of reviewing the extent to which the targets have been achieved. These measures could include:

a. MEASURES

1. Time budget – the work to be done as soon as practicable.
2. Timeframe – the due date should be kept under review.
3. Qualitative – all key areas in line with professional audit standards should be covered.
4. Acceptable – the draft manual should be accepted by audit management.
5. Implemented – plan to get the document implemented should be drawn up and achieved.

b. MEASURES

1. Time budget – one-third of work should be done by 33 hours, one-half by 50 hours etc.
2. Timeframe – the due date should be kept under review.
3. Qualitative – all key areas in line with professional audit standards should be covered.
4. Acceptable – the draft manual should be prepared quickly.
5. Implemented – plan to get the document implemented should be drawn up and achieved.

c. MEASURES

1. Time budget – one-third of work should be done by 33 hours, one-half by 50 hours etc.
2. Timeframe – the due date should be kept under review.
3. Qualitative – most areas should be covered.
4. Acceptable – the draft manual should be accepted by audit management.
5. Implemented – plan to get the document implemented should be drawn up and achieved.

d. MEASURES

1. Time budget – one-third of work should be done by 33 hours, one-half by 50 hours etc.
2. Timeframe – the due date should be kept under review.
3. Qualitative – all key areas in line with professional audit standards should be covered.
4. Acceptable – the draft manual should be accepted by audit management.
5. Implemented – plan to get the document implemented should be drawn up and achieved.

8.14 Which statement is least appropriate?

Even where a time monitoring system is in place, there may still be excess hours charged to jobs. This occurs where:

a. The budget was not set properly.
b. The budget is not seen as a serious issue.
c. Authorization was not secured for extended hours.
d. The audit entailed resolving unforeseen problems and/or difficulties.
e. The client asked for additional work.
f. The auditor decided to do less work.
g. The auditor was 'dumping' time into the job; not all charged hours were worked on the project.
h. The auditor was inefficient.
i. The audit manager caused extra hours to be charged by excessive intervention or lack of it.

8.15 Which paragraph is most appropriate?

a. Findings from internal audit reports and files play an important role. It is insulting to produce a report for management that only has supporting documentation prepared for general impressions. Even where the report is accepted by management, we should be able to confirm all important material that has been reported.
b. Findings from internal audit reports and files play an important role. It is insulting to produce a report for management that has no clear supporting documentation prepared to defined standards. Even where the report is accepted by management, we should be able to confirm all detailed assumptions have been reported.
c. Findings from internal audit reports and files play a less important role. It is insulting to produce a report for management that has no clear supporting documentation prepared to defined standards. Even where the report is accepted by management, we should be able to confirm all important material that has been reported.
d. Findings from internal audit reports and files play an important role. It is insulting to produce a report for management that has no clear supporting documentation prepared to defined standards. Even where the report is accepted by management, we should be able to confirm all important material that has been reported.

8.16 Which statement is least appropriate?

A loss of direction can be the difference between a good audit and a boring report. Demotivated auditors are a problem for audit management even where they do their

work and keep within budget. They will not contribute to the development of the audit function nor inspire others to produce excellent work. Admittedly some auditors cannot be motivated. The CAE should:

a. Prepare and implement an audit strategy that pushes internal audit from one period to another.
b. Publicize this strategy and seek support from staff by instructing them to adhere to it.
c. Market internal audit and recognize achievement so that staff can relate to success criteria.
d. Implement suitable HRM policies and programmes.
e. Remove blockages to performance, particularly with awkward clients who may impair audit's right of unrestricted access to documents, records and information.
f. Keep internal audit fresh and vibrant by regular section meetings, days out, seminars, social events and an invigorating audit manual.
g. Have clear goals.

8.17 Which statement is least appropriate?

Another weakness is lack of follow-up procedures. Auditors adopt the attitude that they do the audit and simply walk away. The follow-up procedure is less of a formality and more an acceptance of responsibility for the audit. The internal auditor needs to:

a. Target high-risk systems.
b. Review the adequacy and effectiveness of the systems of control that protect this system.
c. Alert management to any problems with these controls where necessary.
d. Advise management of ways that systems of control may be improved to handle risk.
e. Ensure management responds to audit findings and indicates what it intends to do.
f. Accept that management will probably take the appropriate action.
g. Revisit the audit after a suitable period to highlight further action management needs to take in respect of its controls.

8.18 Place the following planning tasks (a–f) in chronological order, with the suggested months for each annual activity:

The planning timetable needs to be both fixed and flexible to take on board new developments. One planning system in use follows the pattern below:

a. Analyse information and talk to senior management and the board and decide whether to carry out any relevant consulting projects that are requested by management.
b. Draft risk assessment forms and review of corporate risk database. One audit team uses the following allocations of productive audit time that is assigned in outline to: 50% annual audit plan, 20% emerging risk issues, 7% special investigations, 20% special projects and 3% follow up.
c. Finalize the annual audit plan and discuss with audit committee.
d. Plan is now ready to be implemented.
e. Publish the plan and allow update facilities.
f. Start the new planning process and build in extra capacity for consulting requests for management (via a formal assessment criterion).

8.19 Insert the missing word:

The level of ..... depends on the type of work and auditors employed. For more senior staff, this may be based mainly around the final review procedure, with little involvement from audit management during field work. For less senior staff, a lead auditor may be appointed or the audit manager may spend time with auditors on site. The amount of ..... should correspond with the need to exercise close control over the project.

a. participation

b. motivation
c. performance appraisal
d. supervision

8.20 Which statement is least appropriate?
Audit management must avoid delays in releasing the draft audit report by using the following approach:
a. Introduce technology to ensure reports can be prepared, copied and quickly bound in-house.
b. Set clear reporting standards so that structure and style are not re-invented for every draft.
c. Adopt standardized working papers to feed smoothly into the reporting system. Link papers to show terms of reference, findings, implications, conclusions, recommendations, client comment and agreed-upon action in a logical order that fits the report structure.
d. Write most of the report at the client premises as the audit progresses using laptops.
e. Set separate budgets for the reporting stage that are carefully monitored and controlled.
f. Set a reporting date standard of say five weeks after completion of the fieldwork.
g. Ensure the audit review process is ongoing and does not hold up progress of the draft report.
h. Ensure auditors receive training in efficient report writing and drafting.

8.21 Insert the missing words:
We have moved on from internal audit rubber stamping parts of the system and being part of line operations. The problems are more subtle now where although removed from line roles, internal audit is still locked into the system. This occurs where managers refer their problems to the auditors for resolution. It may be a list of system errors, a breach of procedure or waste occurrence. Taking responsibility away from management and locating this with internal audit gives the auditor . . . . . .
a. more responsibility
b. a better defined responsibility
c. an enhanced status
d. operational responsibility

8.22 Which statement is most appropriate?
Our definition of the audit manual is:
a. A report that involves the accumulation and dissemination of all those documents, guidance, direction and instructions issued by audit management that affect the way the audit service is delivered.
b. A document that involves the accumulation and dissemination of all those documents, guidance, direction and instructions issued by audit management that affect the way the audit service is delivered.
c. A device that involves the accumulation and dissemination of all those documents, guidance, direction and instructions issued by audit management that affect the way the audit service is managed.
d. A device that involves the accumulation and dissemination of all those documents, guidance, direction and instructions issued by audit management that affect the way the auditor behaves.

8.23 Which statement is least appropriate?
Audit manuals fulfil the following roles:
a. Defining standards and methods of work.
b. Communicating this to auditors.

c. Establishing a base from which to measure the expected standards of performance.
d. Providing a mechanism for communicating the audit role to management.

8.24 Which statement is least appropriate?

There is an abundance of material on the advantages of standardization and a number of features can be highlighted:

a. The most familiar standardized procedures are in the form of internal control questionnaires and audit programmes that are developed by many audit departments.
b. Flowcharts should follow a uniform pattern that should be consistently applied throughout the audit department.
c. Standardization leads to consistency and report writing can have a 'house style'.
d. Standardization can lead to auditors giving less attention to format and procedures and more attention to the actual objectives of the task at hand.
e. Standardization means there is more scope for flexibility.
f. Standardization can constitute a vital control over each audit assignment.

8.25 Insert the missing words:

The ..... is the device that allows audit management to consider, formulate and apply suitable audit procedures aimed at ensuring efficiency as well as compliance with standards. It is difficult to visualize any other way that this could be achieved.

a. audit manager
b. audit manual
c. working file
d. working rules

8.26 Insert the missing word:

There appears to be a direct conflict between the extent of direction and standardization that a comprehensive audit manual provides, and the auditor's professional ..... Both are essential for enhancing audit productivity.

a. status
b. standing
c. autonomy
d. competence

8.27 Which statement is least appropriate?

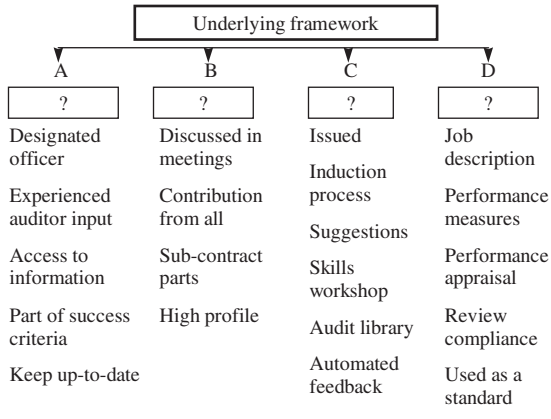
The extent to which the audit manual is kept up to date is one measure of efficiency. Procedures must be completely relevant or they will not be complied with. If not:

a. It gives out signals that the manual is not considered important by audit management and lowers its status. The objective of the document is to reflect and reinforce changing best professional practice.
b. It is easier to insist on compliance and ensure auditors do not drift into their own interpretations of the audit role.
c. It becomes a procedures document held in a rarely used filing cabinet. Important new events that affect the future of internal audit will certainly be addressed by audit management. If they are left out of the manual, it sends the message that the manual is not meant for real issues. Dusty old rules on time sheets and travel claims may be held unchanged in the manual and we return to the old view of the manual as a set of basic administrative procedures.
d. It means newly appointed audit staff, particularly at manager level, will have no firm commitment to adopt the audit style and methodology or to view the internal standards before accepting appointment. Conflict may arise that leads to a disjointed and

uncoordinated service. The role of the manual in pulling together the audit resource around professional standards is lost.

8.28 Select the most appropriate heading (A, B, C or D) for the four columns of the diagram below which is based on four main planks of the audit manual process:

Framework for successful audit manuals



A–D headings: **Insert A, B, C, or D**

1. It must play a role in evaluating auditor's performance
2. The manual has to be used by auditors
3. The task has to be properly resourced
4. The wide concept of the manual has to be supported

8.29 Which three statements are least appropriate?

We want to move towards our target position by developing the 'professional auditor':

a. Ensure that very comprehensive guidance is always provided.
b. Leave general reference material outside the main audit manual.
c. Indicate whether a particular procedure is optional.
d. Explain why a procedure has been selected.
e. Do not allow any departures from the manual.
f. Encourage all auditors to participate in improving the manual and consider rotating the task of maintaining it.
g. Do not appoint an auditor until the approach and standards are explained and he/she can work within them.
h. Where a requirement in the manual has been overridden consider whether an amendment is required.
i. Ensure that auditors who refuse to perform to the requirements of the manual are promoted.
j. Test each section that is drafted to ensure that it is not unnecessarily cumbersome and bureaucratic.
k. Watch out for auditors who appear demotivated and investigate underlying reasons.
l. Ensure that there is a continuous programme to search for and amend all faults.

8.30 Which statement is most appropriate?

a. The audit manual should be a dynamic mechanism for directing auditors and as such represents standard best practice. Accordingly there should be no need to make regular changes either adding to the material in the manual or amending sections.

b. The audit manual should be a dynamic mechanism for directing auditors and as such is ever changing to reflect the latest circumstances and strategy. Accordingly there should be regular changes either adding to the material in the manual or amending sections, and these changes should be drafted by audit management.
c. The audit manual should be a dynamic mechanism for directing auditors and as such is ever changing to reflect the latest circumstances and strategy. Accordingly there should be weekly changes either adding to the material in the manual or amending sections, and all should participate.
d. The audit manual should be a dynamic mechanism for directing auditors and as such is ever changing to reflect the latest circumstances and strategy. Accordingly there should be regular changes either adding to the material in the manual or amending sections, and all should participate.

8.31 What is x?

x . . . . . forces management to set clear objectives and develop their staff. Senior auditors may spend hours on an obscure project that provides no end-product. x . . . . . creates the drive for the audit manager to define and communicate exactly what is to be achieved.

a. Delegation
b. Communication
c. Motivation
d. Professionalism

8.32 Select the most appropriate description (a, b or c) for the three terms (1, 2 and 3):

The final view of information is one based on the type of action that it is meant to stimulate, which may be classified in the following manner:

Term	**Description (a, b, or c)**
1. Strategic	
2. Managerial	
3. Operational	

Descriptions:

a. Weekly time sheets, if processed properly, will generate weekly reports that may be used to get a fix on the performance of audits and auditors. These reports will be more detailed and give the narrow and more accurate picture that is required to make quick decisions on resourcing all current audits. We may wish to abort audits, extend them, transfer resources and/or seek explanation from the field auditor on receipt of this type of information as part of the management process. **Managerial**.
b. Audit management requires aggregate information, say monthly, that sets the global position over the entire audit function for long-term planning. This 'big picture' will assist in the overall direction of audit and help develop a futuristic strategy to cater for the next months or years. **Strategic**.
c. Daily feedback on what is going on in internal audit is one way of controlling resources. This may be related to information on who is doing what, where, for how long and why, so that relevant decisions may be made as required. **Operational**.

8.33 List five attributes of good information:

1.
2.
3.
4.
5.

8.34 Which statement is least appropriate?

Any auditor time monitoring coding system must be based on clear rules that will vary between different audit sections – some general observations:

a. Code the work in line with the adopted reporting framework. The audit committee may have a view on this. In this way, we may secure reports that feed naturally into our monthly, quarterly and annual reporting structures.
b. Make sure all audit work has an individual job code regardless of how long each job takes. It is best not to use general codes such as 'advice' and 'information'.
c. Following this line, it is as well to have small number of fixed codes for non-recoverable (or non-chargeable) time such as annual leave, training, sickness and so on.
d. Have strict rules on who can set up codes and budget hours. This should be restricted to senior staff (say the audit manager or the CAE in smaller audit units).
e. Ensure that time sheets are signed on a weekly basis by audit management before submission to the system.

8.35 Which two statements are least appropriate?

The situation where a newly formed internal audit function has to be developed is not unusual and key issues include:

a. The Audit charter: This sets out the role and objectives of internal audit and is at the core of the delivery of audit services. This is the starting place for a new audit function.
b. Audit standards: The CAE has to decide on two types of standards before the new audit function can be developed – professional and operational standards. The former may be based on those provided by a professional auditing body. Operational standards are more readily achievable since they represent a local interpretation of the professional base.
c. The code of conduct: Another consideration when setting up a new audit service is whether to set standards of conduct before recruiting staff. This is an ideal opportunity where people join only if they feel they can meet the high standards. Once in post, it is difficult to impose new requirements.
d. Recruitment and selection: It is essential that the 'rounded person' is acquired with a whole package of attributes. Training can only go so far, and we are not talking only about formal qualifications and experience.
e. Training: A training budget is essential for the newly formed internal audit unit. This should cover the types of training that will be undertaken for any junior staff who are being employed.
f. The business risk assessment: This is an important part of the development of a new audit function. The general risk survey represents the justification for the new service in that it defines those areas that should be subject to audit coverage.
g. Information systems (IS) audit: One matter that should be high on the agenda for the CAE when designing the new internal audit service relates to computer audit.
h. Fraud work: There is a need to define a clear policy on the detection and investigation of fraud and irregularities.
i. Business planning: The new CAE should devise and publish a business plan that covers the internal audit unit.
j. Assurance and consulting services: One question to be tackled early on in the life of the newly formed unit is related to the type of services that will be provided by internal audit.
k. Budgets: While the CAE must seek to negotiate a large budget, there is great scope to secure extensive funding at the outset.

l. The launch of the new service: The new service must be introduced to the organization. All the well-known devices that this entails should be applied. A good way to do this is to undertake presentations to senior management and the audit committee as well as preparing the all-important audit brochure and web-based facility.

m. The audit manual: We have kept the audit manual as the last topic to be dealt with when setting up a new internal audit department. The extreme view of the audit manual is that of a process that forces audit management to document its objectives, policies and procedures in a formal and publicized fashion.

8.36 Insert the missing words:

Some internal audit shops are turning towards a partnering arrangement, where they use parts of an external firm's expertise to fill in the gaps between strategic requirements and current capacity. This '. . . . . ' model has various positives as well as various negatives.

a. sharing and caring
b. outsourcing
c. co-sourcing
d. contracting-out

8.37 Which four statements are least appropriate?

There are several hot tips for organizations when going to the market for competitive bid including the following:

a. Make a good business case for the contract.
b. Be clear about the solution being offered by the firms and how they add value to the organization's strategy.
c. Engage with the firms early on when developing a specification that bidders can work with to encourage a good number of bids.
d. Select people you can work with so look at behavioural issues and whether the bidders are convincing and engender mutual respect.
e. Ensure strict compliance with the legal contract and instigate all contract penalties involved.
f. Do not miss the big picture in contract monitoring – look at outputs, outcomes and pick up real issues.
g. Make sure there are clear demarcations between client and contractor roles and seek to reinforce these distinctions at all times.
h. Ensure all draft reports go to the CAE before sending out to client.
i. Establish KPIs for the supplier and make them sensible and workable.
j. Place a lot of reliance on post-audit customer questionnaires that go directly to the CAE.
k. Keep the focus on inputs such as the cost of each audit and the time allowed.
l. Make sure the coverage is risk based in line with the corporate risk register.
m. Think about access to expertise in areas such as HR, performance management, compliance work, control awareness, E-business and security that can be obtained at favourable rates from the provider.
n. Find out where CSA fits in and whether this can occur before an audit to focus the audit work.
o. Define clear shortlisting criteria covering such considerations as client references, relevant experience, size and structure of firm, technical/professional capacity, professional conduct and so on.

p. Set values in the contract such as: has the right set of objectives that meet corporate priorities, know what customers want and need from the service, be provided at best value for money and with maximum impact, adds value to the organization.
q. Make reference to meeting the requirements of professional standards such as those issued by the IIA, due professional care requirements and quality assurance models.
r. Mention integration of audit process with the organization's performance initiatives, risk management, E-business, anti-fraud measures, ad hoc demand led work, communicating and consulting with users and regulators and making presentations to the audit committee.
s. Make specific demands such as that the supplier brings an appropriate mix of skills with continuity and stability of staff working on the contract and brings innovations to the service, e.g. CRSA, audit automation and modern data interrogation.
t. Make it clear that only randomly sampled files and working papers are accessible on request by the client.
u. Mention audit approaches (e.g. risk-based systems audits) and criteria for determining testing levels.

8.38 Which statement is least appropriate?

The main steps in the overall planning process are noted below:



Some explanations follow:

a. Organizational objectives. The starting place for audit planning must be in the objectives of the organization. If these objectives are based on devolution of corporate services to business units, then the audit mission must also be so derived. Management must clarify goals and aspirations before plans can be formulated and this feedback can be achieved by active liaison and communication.

b. Assess risk priorities. The relative risks of each audit area must be identified, with reference to the corporate risk database.

c. Resource prioritized areas. Suitable resources for these areas must be provided.

d. Audit strategic plan. A plan to reconcile workload with existing resources should be developed. This should take on board the various constraints and opportunities that are influential now and in the future. The strategic plan takes us from where we are to where we wish to be over a defined time-frame, having due regard for the audit budget.

e. Annual audit plan. A formal audit plan for the year ahead is expected by most audit committees.

f. Quarterly audit plan. A quarterly plan can be derived from the annual plan. Most organizations experience constant change making the quarter a suitable time slot for supportive work programmes.

g. Outline objectives statement. Audit management can make a one line statement of expectations from an audit from work done so far by setting out the final terms of reference and scope for the audit in question.

h. Preliminary survey. Background research requires thought on key areas to be covered in an audit. This ranges from a quick look at previous files and a conversation with an operational manager to formal processes of many days of background work involving a full assessment of local business risks.

i. Assignment plan. We can now draft an assignment plan with formal terms of reference, including budgets, due dates and an audit programme.

j. The audit. Progress should be monitored with all matters in the terms of reference considered.

k. The reporting process. Planning feeds naturally into reporting so long as we have made proper reference to our plans throughout the course of the audit.

8.39 Which statement is least appropriate?

The features of a corporate risk assessment for audit planning include the following:

a. Meeting with managers is an opportunity not only to get to know them but also to introduce the audit role to clients and gain an appreciation of their concerns.

b. It provides material to establish the real risks facing the organization.

c. A useful side effect of the risk review is that link officers may be established in each department/division to provide a vital communication device between the audit field and management.

d. This close contact enables the auditor to follow up on matters that have been reported previously and get updates on progress in making required improvements to controls.

e. The main objective of audit planning is to provide input to the risk assessment process so that any improvements to risk management may be provided by management and then reported back to the audit committee.

f. There is the opportunity to listen to managers, on the basis that 'listening' is a dynamic technique based around interactive communications.

g. The part of the risk review process that involves meeting with management is aided through questionnaires and checklists, which shorten the interview process.

h. Auditors should be given specific areas in the organization that they will have responsibility for and then be charged with securing information on them.

i. A filing system can hold the database of information and so smooth the survey data.

j. The risk review brings management into the planning process and ensures that audit plans are based on the best up-to-date information.

k. While the risk review may be based around meetings with management and reviewing information supplied to internal audit, there must be an element of independence in the way this information is procured and used.

8.40 Insert the missing words:

Audit will be required to publish an annual audit plan formally approved by the .....

a. chief executive officer

b. CAE

c. senior management
d. audit committee

8.41 Which statement is least appropriate?

Some of the features of the annual audit plan are as follows:

a. It contains key audit areas for the next 12 months and explains why they were selected through a suitable preamble.
b. Following from the above, the annual plan needs to be interfaced with the annual report.
c. The plan itself should be circulated to the directors for their consideration and approval before being finalized.
d. Once top management has seen the plan, it will be presented to the audit committee to be formally adopted. Changes to the plan should likewise be confirmed at audit committee.

8.42 Insert the missing words:

Many internal audit shops have moved on from the risk assessment checklists and entered into a ..... about how the audit resource can be used to the best effect, that is, utilizing the corporate assessment of risks along with auditor's special expertise in risk management, control models and specific control mechanisms (and requests for consulting projects).

a. scientific appraisal
b. dialogue with the board
c. dialogue with the entire audit team
d. general estimation

References

1. *Financial Mail on Sunday*, 22 Sept. 2002, p. 4, 'Why can't he be forced to pay the price of failure', Laurence Ben.
2. Willey Peter, 'A strategy focus'. *Internal Auditing*, July 2000, p. 14.
3. Roth James (2002) *Adding Value, Seven Roads to Success*, Orlando: IIA.Inc.
4. White Scott, Fuller Walter and Dugan Timothy, 'Unchartered waters'. *Internal Auditor*, Feb. 1999, pp. 55–58.
5. Summerell Mike, *Internal Auditor*, Feb. 2000, In My Opinion, p. 96.
6. Moeller Robert and Witt Herbert (1999) *Brink's Modern Internal Auditing*, 5th edition, Para. 8.16, New York: John Wiley and Sons Inc.
7. Moeller Robert and Witt Herbert (1999) *Brink's Modern Internal Auditing*, 5th edition, New York: John Wiley and Sons Inc., p. 494.
8. Chapman Christy and Anderson Urton, IIA (2002) 'Implementing the professional practices framework', in The IIA Handbook Series, p. 91.
9. Leithhead Barry S. (ed.) Dec. 2000, 'In touch with the top'. *Internal Auditor*, p. 67.
10. Professor Marchant Garry 'Strategic performance measurement'. *Accounting and Business*, May 1998.
11. 'Getting the balance right'. *Internal Auditing and Business Risk*, June 2000, pp. 20–22, IIA.UK Survey of Almost 200 Audit Functions on Some Key Benchmarking Measures – The Institute's Benchmarking Survey.
12. Balanced Scorecard, 'Applying and implementing the balanced scorecard'. Society of Management Accountants of Canada, 1999, p. 12.
13. Moeller Robert and Witt Herbert (1999) *Brink's Modern Internal Auditing*, 5th edition, New York: John Wiley and Sons Inc., p. 497.
14. IIA.Inc., *Professional Practices Pamphlet*, 1998-1, A Perspective on Outsourcing of the Internal Audit Function, p. 12, Internal Auditing: The Long-Run Approach.
15. Smith Paul J. Jr, 'Win-win cosourcing'. *Internal Auditing*, Oct. 2002, pp. 37–41.
16. The IIA, 'The outsourcing dilemma: what's best for internal auditing', Rittenberg Larry E. and Covaleski Mark A. (1998).

17. Lapelosa Michael, 'Outsourcing – a vulnerability checklist'. *Internal Auditor*, Dec. 1997, pp. 66–67.
18. Rittenberg Larry and Covaleski Mark, 'Study – the outsourcing dilemma: what's best for internal auditing', Sponsored by The IIA Research Foundation, *Internal Auditing*, May 1998, p. 77.
19. Cowan Neil 'Challenging internal audit (outsourcing)'. *Internal Auditing*, Sept. 1991.
20. Wills Steve, 'Internal auditing and business risk', Sept. 1999, pp. 13–15.
21. O'Regan David, in The IIA 2002, The IIA Handbook Series, *Strategies for Small Audit Shops*, p. 22.
22. Hubbard Larry 'Audit planning'. *Internal Auditor*, Aug. 2000, pp. 20–21.
23. AUDIT COMMITTEE BRIEFING (2006) *Internal Audit Standards: Why They Matter*, Institute of Internal Auditors, August 2006.
24. Chief Audit Executives and Audit Committees: Building A Strong Relationship, pp. 4–10, This report highlights the results of a survey, designed and conducted by Crowe Horwath LLP to better understand the relationship between chief audit executives and audit committees, Executive Summary, 2008 Crowe Horwath LLP.
25. Chief Audit Executives and Audit Committees: Building A Strong Relationship, pp. 4–10, This report highlights the results of a survey, designed and conducted by Crowe Horwath LLP to better understand the relationship between chief audit executives and audit committees, Conclusions and Recommendations, 2008 Crowe Horwath LLP.
26. Internal Auditing & Business Risk, IIA Magazine, Fair but firm, pp. 12–17, October 2008, Rosemary Hilary talks to Neil Baker about the changes she's been making to the internal audit function at the FSA, and her report on the demise of Northern Rock.
27. Internal Auditing & Business Risk, IIA Magazine, August 2007, pp. 36–37, Hanif Barma.
28. Internal Auditing & Business Risk, IIA Magazine, July 2007, John Buchanan tells Neil Baker what he looks for in a head of internal audit, pp. 17.
29. Business upheaval: Internal audit weighs its role amid the recession and evolving enterprise risks, p. 7, PricewaterhouseCoopers 2009, State of the internal audit profession study, PricewaterhouseCoopers' fifth annual state of the internal audit profession.
30. Prescriptive Guide Series Operational Excellence: Linking Your Business, Compliance, Operations and Security, p. 25. Tripwire Inc, 2005.
31. An opportunity for transformation, How internal audit helps contribute to shareholder value, p. 9, Pricewaterhouse Coopers, October 2008.
32. An opportunity for transformation, How internal audit helps contribute to shareholder value, p. 27, Pricewaterhouse Coopers, October 2008.
33. Internal Auditing & Business Risk, IIA Magazine, May 2009, Internal Auditing, p. 35, Steven Shackleford and Richard Hollands.
34. Internal Auditing & Business Risk, IIA Magazine, pp. 25–26, October 2009, Dave Corbin?
35. Internal Auditing & Business Risk, IIA Magazine, July 2008, p. 28, Why internal audit matters, Paul Boyle tells Neil Baker.
36. Internal Auditing & Business Risk, IIA Magazine, July 2008, p. 30, Why internal audit matters, Paul Boyle tells Neil Baker.
37. Roth James (2002) *Adding Value, Seven Roads to Success*, IIA Research Foundation.

Chapter 9

AUDIT FIELD WORK

Introduction

We have established that there are many different interpretations of the internal audit role and many approaches to performing both assurance and consulting work. One basic approach that has been discussed is risk-based systems auditing. This involves establishing the system objectives, finding out what risks should be addressed and then developing appropriate solutions to mitigate unacceptable levels of risk. The audit can be done by the client (with help from internal audit), by the auditor but with a great deal of participation with the client, or entirely by the internal auditor (as an outsider). These perspectives form a spectrum from objective review through to facilitated self-assessment. Whatever the adopted format, the auditor should perform field work to arrive at an opinion and advise on managing outstanding risks. Apart from the self-assessment approach, which is more consultancy than anything else, the internal auditor may go through variations on several set stages in performing the audit. Note that all references to IIA definitions, code of ethics, IIA attribute and performance standards, practice advisories and practice guides relate to the IPPF prepared by the Institute of Internal Auditors in 2009. The various stages for performing an audit are covered in this chapter and include:

9.1 Planning the Audit
9.2 Interviewing Skills
9.3 Ascertaining the System
9.4 Evaluation
9.5 Testing Strategies
9.6 Evidence and Working Papers
9.7 Statistical Sampling
9.8 Reporting Results of the Audit
9.9 Formal Presentations
9.10 Audit Committee Reporting
9.11 New Developments
Summary and Conclusions
Assignments and Multi-choice Questions

9.1 Planning the Audit

The annual audit plan lists those high-risk areas that are targeted for audit cover during the next 12 months. The quarterly audit plan provides more detail by setting out those audits that will be performed by specified auditors in the following three months. Before the full audit is started and resources committed, an assignment plan will direct and control these resources. Before we are in a position to formulate assignment plans, we need background information on the targeted operation. Preliminary work will be required, the extent of which will vary according to the size

of the audit. This section sets out the principles behind the preliminary survey and assignment planning, although the approach and level of detail will vary depending on the policies of each individual audit department. The IIA Performance Standard 2200 deals with engagement planning and requires that:

> Internal auditors must develop and document a plan for each engagement, including the engagement's objectives, scope, timing, and resource allocations.

The Preliminary Survey

The preliminary survey seeks to accumulate relevant information regarding the operation under review so that a defined direction of the ensuing audit (if it goes ahead) may be agreed. The internal audit files will be the first port of call and any previous audit cover will be considered. All assignment audit files should contain a paper titled 'Outstanding Matters' that will set out concerns that were not addressed via the audit at hand. The files tell only part of the story as will the resultant audit report, and it is best to talk to the auditor who last performed work in the relevant area. It is advisable to carry out background research into the area subject to the survey. This might include national research, committee papers, recent changes and planned computerized systems. Much of this information should really have been obtained via the corporate risk assessment. It is always advisable to get some basic facts before meeting with management so as to create a good impression. We can now meet with the key manager and tour the operational area. An overview of the real risks facing the manager in question can be obtained. A feel for the audit can be gathered from impressions gained from touring the work area, where the initial impression can be used to help direct the auditor towards particular problems. A checklist of matters to be covered in such an opening meeting should be drafted to form the basis of the discussions, covering items such as:

A. Key control objectives
- The reliability and integrity of information
- Compliance with laws, policies and procedures
- Safeguarding assets
- Economy and efficiency and effectiveness.

B. Key managerial processes
- Operational objectives
- Strategy
- Structure
- Human resource management
- Information systems
- Direction, supervision and procedures.

C. Key risks
- Inherent risks
- Risk assessment undertaken
- Significant risks in terms of impact and likelihood
- Current measures to manage risk including key controls.

Control objectives are the positive things that business managers want to happen rather than negative things they want to prevent happening and they address the risks inherent in the work

being done. Control objectives are used by some auditors to represent a statement of the desired result or purpose to be achieved by the specific control procedures to ensure business objectives are achieved. Once set it is possible to start thinking about the risks to each of the defined control objectives to reinforce the performance/conformance dimensions of acceptable business practices. The drawback is that it is often difficult to sell the idea of control objectives to client management. Note that Performance Standard 2120.A1 reinforces the scope of internal auditing by requiring that:

> The internal audit activity must evaluate risk exposures relating to the organisation's governance, operations and information systems regarding the:
>
> - Reliability and integrity of financial and operational information.
> - Effectiveness and efficiency of operations.
> - Safeguarding of assets.
> - Compliance with laws, regulations, and contracts.

1. Operational procedures Recent work carried out by other review agencies should be obtained and considered, although one should watch out for bias where the work was commissioned for a particular reason. Reports contain natural bias set by the terms of reference. For example, a staffing review commissioned by an employee union is more likely to recommend pay rises. The preliminary survey involves assessing local business risk factors that affect audit objectives. No audit can cover all the relevant areas within a specific operation and the assignment plan states what will be done and what is not covered. It is the process of assessing local risk that allows the auditor to key into the target elements of the operational area. This is done at preliminary survey before the audit objectives and scope of the review can be finalized and agreed upon. The auditor must isolate the system for review and distinguish it from parent systems, subsystems, parallel systems and link systems. Systems theory states that a system is defined in line with the perceptions of the reviewer. The system selected by the auditor has to be defined before it can be audited and the preliminary survey comes to the rescue. Systems boundaries can only be determined after the necessary information has been accumulated and digested. This must happen before the assignment planning stage so that a clear plan may be documented and shown to management. The aim of the preliminary survey will be to agree to the objectives and scope and timing of the audit with management. What needs to be done, how and when it will be done, will be derived from the survey as a prerequisite to the proper preparation for the full audit. It will be necessary to note areas that will be considered as outside the terms of reference. This is important because management often feel that an audit will reveal all that is wrong with a system. A clear definition of what was not included in the audit will help to avoid this. Note that the IIA define engagement objectives as: 'broad statements developed by internal auditors that define intended engagement accomplishments'. A major benefit of the preliminary survey is an understanding of the nature of the audit. This highlights the type of audit skills required, including special skills relating to automation and/or technically complicated matters such as contract law. Audit standards require audit management to ensure they can perform audits to professional standards. It is the responsibility of managers to use their resources properly and if it is clear that an audit is too difficult for the available resources then the project should be aborted. It is a useful policy to get senior auditors or audit managers to perform the preliminary survey and then assign the full audit to more junior staff. The survey is perhaps the most difficult part of the audit process since once the terms of reference have been set and a programme of work agreed upon,

the remainder can be fairly straightforward. It means that the audit manager has full knowledge of the audit and can supervise and review the work as it progresses. The preliminary survey should result in a programme of work that has been identified as a result of the background work. This may be in the form of a detailed audit programme or simply a list of key tasks depending on the type of audit, the approach to work and the policies of the audit unit.

2. The audit programme Besides isolating the system for review and determining the direction of the audit, the assignment plan may result in an audit programme for use during the audit. Performance Standard 2240 mentions work programmes and says that: 'Internal auditors must develop work programs that achieve the engagement objectives. These work programs should be recorded'. And there are separate standards for assurance and consulting work that suggest:

> **2240.A1** – Work programs must include the procedures for identifying, analyzing, evaluating, and documenting information during the engagement. The work program must be approved prior to its implementation, and any adjustments approved promptly.
>
> **2240.C1** – Work programs for consulting engagements may vary in form and content depending upon the nature of the engagement.

The term audit programme (or work programme) should be carefully considered since an audit programme tends to be associated with a series of predefined testing routines. This does not promote the systems-based approach since the direction of the testing procedures depends on the outcome of the risk and control evaluation. The IIA define the engagement work programme as:

> A document that lists the procedures to be followed during an engagement, designed to achieve the engagement plan.

The audit programme may be seen more as an audit guide and may include:

1. Defining the various tasks that need to be performed. Here a list of key tasks should be compiled for the lead auditor that sets the direction of the audit process that will now be carried out. This is not only a useful planning tool that can be used to monitor progress on the audit, but also provides firm guidance for the auditor on work that must be completed.
2. Defining the extent of work in a particular part of the operation. For smaller audits with a probity approach it is possible to list the various testing routines. Defining testing programmes makes the audit controllable. It is based around the required tests and in basic audits this may give the number of items that should be selected and how they are tested. Audit management can exercise firm control. This would not be appropriate for a systems-based approach since it is controls that are tested after they have been assessed and testing is not carried out for its own sake.

The key differences between the systems and compliance/probity approaches to audit work are found in Figure 9.1.

This is an important distinction. Compliance and probity audits emphasize transactions testing, and the audit programme is formulated at the preliminary survey stage. For systems audit this detailed testing programme can only be defined after the system has been documented and assessed. The programme of work that is set for a systems audit can be described as an audit guide that determines the work required to complete the audit and this may be drafted at the

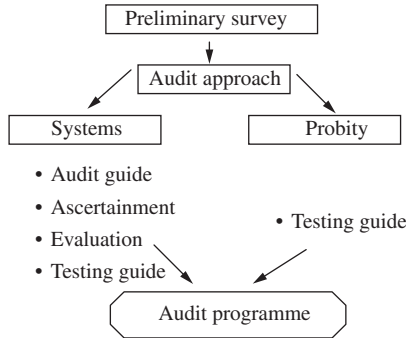


FIGURE 9.1 Systems-based approach versus probity.

preliminary stage. The programme will include target dates and perhaps a progress checklist for stages of the audit. Not only is it used as a monitoring tool but as each task is carried out, the date completed and reviewed should be entered on the schedule and this provides a comprehensive record of the work. The audit techniques may be identified and this may affect the type of auditors that need to be assigned. Statistical sampling, flowcharting, interviewing, computer assisted audit techniques, product inspection, third-party circularization and other techniques may be planned where clearly required. Resourcing these techniques can be dealt with at the pre-planning stage. If the requisite skills are not available, audit management must secure them or suspend/abort the audit. The audit programme should be formally signed off by the audit manager to constitute an approved work plan for the field auditor/s. Attaching the programme to the associated terms of reference and budget for the work provides a management tool for controlling the audit. The audit programme sets direction for the testing stage, but care must be taken not to suppress the auditor's initiative or responsibility for the work. There must be direction but at the same time freedom to explore key issues and form an opinion on the state of controls. For systems audits, the test programme appears after most of the crucial evaluation work has been completed. For compliance audits it is essential that the auditor uses the programme as a means to an end and not an end in itself. This means tailoring the programme to fit the audit while retaining responsibility for the end results. Where the audit is being driven by the audit programme, then it is necessary to make clear the tasks that need to be carried out. Sawyer has suggested a series of formal definitions of tasks to help eliminate confusion between the audit programme writer and the staff auditor:

- Analyse – To break into significant component parts and determine the nature of something.
- Check – To compare or recalculate, as necessary, to establish accuracy or reasonableness.
- Confirm – To prove to be true or accurate, usually by written inquiry or by inspection.
- Evaluate – To reach a conclusion as to worth, effectiveness or usefulness.
- Examine – To look at or into closely and carefully for the purpose of arriving at accurate, proper and appropriate opinions.
- Inspect – To examine physically.
- Investigate – To ascertain facts about suspected or alleged conditions.
- Review – To study critically.
- Scan – To look over rapidly for the purpose of testing general conformity to pattern, noting apparent irregularities, unusual items or other circumstances appearing to require further study.
- Substantiate – To prove conclusively.

- Test – To examine representative items or samples for the purpose of arriving at a conclusion regarding the population from which the sample is selected.
- Verify – To establish accuracy.

The term audit is too general to use in referring to a work step.[1]

3. The preliminary survey report It is advisable to present a formal preliminary survey report (PSR) once the work has been completed. Another consideration is that access to information and explanations is important to establish at an early stage and help is given here by various elements of performance Standard 2220:

> **2220.A1** – The scope of the engagement must include consideration of relevant systems, records, personnel and physical properties, including those under the control of third parties.
>
> **2220.A2** – If significant consulting opportunities arise during an assurance engagement, a specific written understanding as to the objectives, scope, respective responsibilities and other expectations should be reached and the results of the consulting engagement communicated in accordance with consulting standards.
>
> **2220.C1** – In performing consulting engagements, internal auditors must ensure that the scope of the engagement is sufficient to address the agreed-upon objectives. If internal auditors develop reservations about the scope during the engagement, these reservations must be discussed with the client to determine whether to continue with the engagement.

The PSR goes to the audit manager, along with a brief description of the system to be used to prepare the assignment plan. The PSR of one or two pages will cover the following:

1. An outline of the system under review including systems objectives and boundaries.
2. The work undertaken in the preliminary survey.
3. An initial opinion on the risk areas based on the key control objectives covering compliance, information systems, safeguarding assets and VFM.
4. Recommendations for the proposed assignment in terms of the nature and extent of audit cover now required.
5. An appendix with outline systems notes and a draft audit guide/programme for the full audit.

Assignment Planning

Each audit must be carefully planned as this is the only way to control it. Assignment planning takes all available information and allows the objectives, scope, direction and approach to be defined. The preliminary survey will have been conducted before plans can be formulated and will provide much information for formulating the assignment plan. The preliminary survey report will set out the proposed objectives of the full audit stage. Factors to be addressed in the assignment plan are:

1. The terms of reference for the audit by audit management, which are disclosed to the client management. They guide audit work and feature in the resultant report with an audit opinion on each component. The precise terms of the audit should be given much consideration in line with Performance Standard 2220, which says: 'The established scope must be sufficient to satisfy the objectives of the engagement'.

2. The scope of work including areas for coverage and parts of the system not to be dealt with at this time. This may be referred to in a memorandum to client management publicizing the pending audit.
3. Target dates for start and completion and key stages. For larger audits, the task should be broken down into defined stages. The audit should be sectioned into manageable parts that may be reported on separately. This enables the auditor to maintain a focus on the objective at hand, and report before going on to deal with the next part. For example, a corporate system, which has been devolved down to departments like personnel, budgeting, or expenditure processing, may be broken down into sections relating to each department. A separate report will be drafted for each department along with a composite report covering the corporate arrangements. Auditors can be drafted in to deal with each department if a suitable programme of work has been prepared and explained since the work programme requires extensive testing and interrogation of the corporate database. Once compiled, it can be completed by a variety of resources including temporary audit staff. Practice Advisory 2230-1 acknowledges that auditors may have development needs and suggests that: internal auditors consider the following when determining the appropriateness and sufficiency of resources:
   - the number and experience level of the internal audit staff;
   - knowledge, skills and other competencies of the internal audit staff when selecting internal auditors for the engagement;
   - availability of external resources where additional knowledge and competencies are required;
   - training needs of internal auditors as each engagement assignment serves as a basis for meeting the internal audit activity's developmental needs.

   Some assistance may be provided by audit management to address any particular problems experienced by the field auditor. This may include any follow-up action taken on an audit report issued previously that impacts on the audit. The auditor will also be concerned that compliance issues have been addressed by management and Performance Standard 2210.A2 covers this point by commenting that: 'The internal auditor must consider the probability of significant errors, irregularities, noncompliance, and other exposures when developing the engagement objectives'.
4. A full definition of the system under review including the points where it starts and finishes and interfaces with other related systems. This avoids unnecessary confusion over the duration of the audit with a clear focus on exactly what the system is. It allows the auditor to think through the associated systems and their impact on the audit.
5. Identification of risk areas and critical points of the audit that may require special attention and/or resources. This may refer to the timing of the audit, say in relation to restructuring, a new computer system, a recruitment campaign or a new staff performance scheme. On this point, Performance 2210.A1 says – 'Internal auditors must conduct a preliminary assessment of the risks relevant to the activity under review. Engagement objectives must reflect the results of this assessment'. On the other hand, consulting engagements are defined by the client and Performance standard **2210.C1** states – 'Consulting engagement objectives must address governance, risk management, and control processes to the extent agreed upon with the client'.
6. Definition of the reporting and review arrangements including a list of the officers who will receive draft reports. Where the audit is geographically remote, the review arrangements must be determined so that this process does not hold up the progress of the audit report.
7. Establishing a confirmed audit programme (or guide) for each part of the audit and the testing regimes (for compliance reviews). The audit techniques that should be applied may also be defined along with a list of standardized documents (having reference to the audit manual) in

use in the audit unit. On this point, Practice Advisory 2240-1 argues that: 'Internal auditors develop and obtain documented approval of work programs before commencing the internal audit engagement. The work program includes methodologies to be used, such as technology-based audit and sampling techniques'. The process of collecting, analyzing, interpreting and documenting information is to be supervised to provide reasonable assurance that engagement objectives are met and that the internal auditor's objectivity is maintained.

8. The assignment plan will outline any travel and hotel arrangements along with subsistence allowances. This should recognize the need to save time and ensure efficient use of resources.
9. Identify the auditors assigned to the project and their roles. Performance Standard 2230 covers resource allocations and states that: 'Internal auditors must determine appropriate and sufficient resources to achieve engagement objectives based on an evaluation of the nature and complexity of each engagement, time constraints, and available resources'. The assignment planning task must identify which auditors are assigned. The audit manager or lead auditor should perform the preliminary survey so that a good insight into the audit is obtained by those directing the work. Once done, the audit proper should be assigned. A trend is for a move away from teamwork with a single auditor being given an audit to streamline resources. It fits with the development profile of auditors who, apart from trainees, should be given responsibility for whole projects. Meanwhile the IIA Performance Standard 2201 provides a list of matters to be considered when planning the audit such as:

    - The objectives of the activity being reviewed and the means by which the activity controls its performance;
    - The significant risks to the activity, its objectives, resources, and operations and the means by which the potential impact of risk is kept to an acceptable level;
    - The adequacy and effectiveness of the activity's risk management and control processes compared to a relevant control framework or model; and
    - The opportunities for making significant improvements to the activity's risk management and control processes.

    Consulting engagements are more straightforward and are covered by Performance Standard 2201.C1, which requires that Internal auditors must establish an understanding with consulting engagement clients about objectives, scope, respective responsibilities and other client expectations. For significant engagements, this understanding must be documented.

Assigning Time Budgets to Audits

We must define an audit budget in terms of time allowed. Time is the key factor in any audit. Setting a time budget acts as a principal control over the assignment and is the single most important concern of audit management. A viable audit is achieved within budget to professional audit standards and as a full discharge of its objectives. Budgeted hours must be realistic and achievable. An alternative approach is more basic and simply states (for example):

LARGE AUDIT:	**4 WEEKS**
MEDIUM-SIZED AUDIT:	**2 WEEKS**
SMALL AUDIT:	**1 WEEK**

The extent of work done in such time frames depends on the skill and expertise of the individual auditor. A performance appraisal scheme rewards those who deliver quality reports within the time constraints. There are two different views. One seeks to perform the audit terms of reference to the full no matter how long this takes, even if budgeted hours are extended. This normally involves extensive testing and an inability to defer parts of the audit to a later stage. The other view is that audit management sets a defined number of hours according to the level of risk attached. When this budget expires the auditor must transfer to another work area, so recognizing the risks of not dealing with the next planned audit. Extensions are not encouraged as the auditor has to perform as much work as possible during the budget hours and then move on to the next job. The adopted policy must be explained and detailed in the audit manual since work done on one audit detracts from work that might be done elsewhere. One solution is to disallow budget extensions unless there is good reason such as to avoid the psychological dilemma of 'auditor attachment'. This occurs where the auditor becomes so engrossed in an operation that he/she sees himself/herself as an expert who has a duty to solve all problems after mastering the system. Client managers assimilate the auditor into an executive role by constantly seeking advice on operational decisions. The auditor becomes too closely associated with the operation, asking for more and more time to spend on the audit. The correct position is to provide budgeted hours for the audit and then remove the auditor from the work once this has expired. The working file will show what work is outstanding that may be deferred to the next audit. Auditor attachment can lead to audit saturation where there has been too much time spent by the audit team on only one area of risk.

1. The assignment planning process The audit manager should provide all guidance in the assignment plan before the full audit commences. Objectives in the assignment plan should be achieved and the audit manager review should ensure this. Performance Standard 2110 makes clear the audit link to corporate governance and states that: 'The engagement's objectives should address the risk, controls and governance processes associated with the activities under review'. The assignment plan should also incorporate review points over audit hours charged and quality of work to judge the value of work performed. Not all requests for formal consulting projects can be accepted by the internal auditor and Performance Standard 2220.C1 makes it clear that some projects will have to be declined by saying that: 'In performing consulting engagements, internal auditors must ensure that the scope of the engagement is sufficient to address the agreed-upon objectives. If internal auditors develop reservations about the scope during the engagement, these reservations must be discussed with the client to determine whether to continue with the engagement'.

2. Planning documentation There are many versions of documents that assist audit planning to provide standards and checklists for the work and areas that should be covered in the plan, showing each task and indicating:

The audit objective	Who does what
For how long	Any particular guidance
The review arrangements	

This control will not work unless there is an in-built monitoring system of continual supervision and review of progress. The audit manager should provide all necessary direction via the assignment planning process. The details above are the minimum information that should be contained in audit plans before the full audit is approved by audit management. Practice Advisory 2010-1 also gives guidance on what should be included in engagement work schedules:

> In developing the internal audit activity's audit plan, many chief audit executives (CAEs) find it useful to first develop or update the audit universe. The audit universe is a list of all the possible audits that could be performed. The CAE may obtain input on the audit universe from senior management and the board.
>
> The audit universe can include components from the organization's strategic plan. By incorporating components of the organization's strategic plan, the audit universe will consider and reflect the overall business' objectives. Strategic plans also likely reflect the organization's attitude toward risk and the degree of difficulty to achieving planned objectives. The audit universe will normally be influenced by the results of the risk management process. The organization's strategic plan considers the environment in which the organization operates. These same environmental factors would likely impact the audit universe and assessment of relative risk.

The CAE prepares the internal audit activity's audit plan based on the audit universe, input from senior management and the board, and an assessment of risk and exposures affecting the organization. Key audit objectives are usually to provide senior management and the board with assurance and information to help them accomplish the organization's objectives, including an assessment of the effectiveness of management's risk management activities.

The audit universe and related audit plan are updated to reflect changes in management direction, objectives, emphasis and focus. It is advisable to assess the audit universe on at least an annual basis to reflect the most current strategies and direction of the organization. In some situations, audit plans may need to be updated more frequently (e.g. quarterly) in response to changes in the organization's business, operations, programs, systems and controls.

Larger Audits

There are times when the internal audit shop is asked to perform a large piece of work and this may take several months to complete. Major change projects such as integrating two large enterprises when a takeover has occurred or budget reduction exercises, or a review of the entire corporate governance arrangements may result in a full-blown audit project that needs to be carefully considered and planned. Some organizations embark on major reform programmes and will establish many individual projects to implement the overall development programme. Where internal audit becomes involved in larger projects, the need for formal project management may be deemed appropriate. Each larger project has its own brief, resource management, risk register, stakeholder communication channels and even a special QA process involving a project board. The other feature is a dedicated project manager with a semi-permanent staff, and administrative support, rather than just a lead auditor and a staff auditor. One useful technique is to perform pilot exercises and review these before carrying out the main programme of work. A financial (and not just time) budget would be provided and an assigned project sponsor will look for regular reports of progress against targets. One popular technique is to install formal checkpoints into the project so that at various stages an independent panel of between two and five specialists will review progress and decide whether they need to 'pull the plug' and stop all further work. A typical gateway project with eight main stages and six gateway reviews may be set up as follows:

1. **Business Strategy**
2. **Establish Business Need**

Gateway Review 0 – strategic assessment.

3. **Develop Business Case**

Gateway Review 1 – business justification.

4. **Develop Procurement Strategy**

Gateway Review 2 – procurement strategy.

5. **Competitive Procurement**

Gateway Review 3 – investment decision.

6. **Award and Implement Contract**

Gateway Review 4 – readiness for service.

7. **Manage Contract**

Gateway Review 5 – benefits evaluation.

8. **Closure**

The audit website may include a running commentary on the project and progress made as a form of communication with the rest of the organization. The project may have its own mission (why we exist), goals (statement of what we want to achieve), objective (one of several things we must achieve to manage our goals) and vision (imaginative and challenging picture of our future).

Driving Internal Audit with Risk Assessments

By Dan Swanson, *Compliance Week Columnist*

For an internal audit function to be effective, its efforts must be risk-based and must meet the organization's long-term assurance requirements. Members of the board, the audit committee and executive management look to internal audit to cover the entire spectrum of risks and issues facing the organization; that is, they expect internal audit to assess the significant risks to the organization and provide timely assurance that adequate controls are operating effectively to mitigate those risks. It is a huge responsibility. Most organizations have numerous potentially auditable entities (corporate initiatives, business lines, systems, regulatory requirements; the list is endless) and internal audit must decide which of these entities they are going to tackle first. The audit risk assessment works to bring at least a semblance of order to the audit universe, evaluating the various possibilities and attempting to address the potential risks facing the organization.

Risk Assessments And Auditing Priorities

The International Standards for the Professional Practice of Internal Auditing as promulgated by the Institute of Internal Auditors specify that:

- The chief audit executive should establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organization's goals (Standard No. 2010 – Planning); and

- The internal audit activity's plan of engagements should be based on a risk assessment undertaken at least annually. The input of senior management and the board should be considered in this process (Standard No. 2010A). That is to say, internal audit plans and priorities must be driven by a risk assessment at both the macro level (for the annual plan) and the micro level (for each audit engagement).

Audit risk assessments come in all shapes and sizes, reflecting the vast diversity of business environments: from very formal, very detailed, annual assessments, to more of a rolling high-level analysis on a quarterly or even monthly basis (even moving to an almost continuous basis for some organizations) with the related audit plans being revised almost as regularly.

To develop an audit plan, the risk assessment evaluates the key forces that create risk for the organization and assesses two fundamental factors:

1. The potential impact of a risk's occurrence, and
2. The likelihood of that occurrence.

Those factors must also be aligned with the business environment in which the organization operates; in other words, they must be relevant. The audit risk assessment is not an end – it is a means to an end. Internal audit needs to define the audit universe and assess the risks facing the organization in achieving its objectives, so that audit efforts can be properly prioritized.

Revisiting the risk assessment regularly helps ensure that the path you take continues to be the right one. After all, mid-course corrections are always needed. Consider a 747 flying from New York to San Francisco. A flight plan is created based on all the factors known prior to leaving New York – which is to say, the risks and requirements are assessed (weather concerns, traffic issues, equipment capabilities, and so forth). Throughout the flight, progress is monitored and mid-flight corrections are made to ensure the flight is efficient and on the right path. Finally, upon arrival, a post-trip evaluation is completed to determine what, if anything, should be changed for the next trip.

Now apply that approach to the world of corporate auditing. What priority should be assigned to an audit of, say, the human resources department's efforts, versus the security system for an organization's numerous inventory warehouses? If the skills and creativity of the organization's workforce truly drive the long-term success of the organization, HR might be the logical target for your next big audit. Conversely, if the products in the warehouse (if compromised) could bring the organization to its knees, then a security audit might be the top priority.

In other words, improving the risk assessment process helps to ensure that audit priorities are appropriate. Many of the resources provided in the sidebar (see box at left) present the consensus views of leaders in internal audit and risk management, and should be evaluated for applicability to your organization. And what if your audit risk assessment is wrong? My answer has always been that it's better to try to forecast the future than just to let it happen to you. Besides, whenever you have analysis and debate about risks – their potential to disrupt, the controls and contingency plans to address them, and so forth – that invariably strengthens the organization. It's just human nature: If you give the auditor and management a flashlight and tell them to look in their closets each year, eventually people starting cleaning those closets up.

Reprinted from *Compliance Week*. This article was originally published in Compliance Week. Reproduced by permission of Compliance Week. All rights reserved.

The Internal Audit Plan as a Roadmap

The end result of the risk assessment process is the internal audit plan. Establishing or updating an internal audit plan is not always easy, but it is critical; without a plan you are not in control. Without an approved plan you also do not have the needed support and (equally important) agreement on what the long-term assurance requirements for the organization truly are. An important issue in developing the internal audit plan is the involvement of management. While the input from management stakeholders is vital, the independent judgement and final decisions need to rest mainly with the CAE. Management cannot dictate audit priorities.

In an established audit function, with many years of experience with audit plans, a meeting with a few executive guests can complete the review and provide a final proposal to the audit committee. At the end of the day, the audit committee (representing the board's many interests) is responsible for approving the CAE's audit plan. Presenting the proposed internal audit plan to the audit committee for approval is one of the most critical activities within internal audit. The audit committee's stamp of approval sets the direction for internal audit's efforts, and facilitates senior executives' debates about:

1. what is really important to the company;
2. what challenges are facing the company; and
3. what the internal audit department believes to be the key risks facing the company.

As corporate governance debates go, they do not get any better than that! Directors must satisfy themselves that the audit plans are appropriate and that internal audit will contribute to the organization's performance results. The dialogue between management, the audit committee and the CAE regarding the audit plan ensures that internal audit has a seat at the governance table. In general, development of an effective audit plan involves a combination of everything talked about today: risk assessment, dialogue among all the key stakeholders, a consensus on what internal audit wants to achieve, and finally, what assurance needs for the organization must be met.

Finally, an approved audit plan is not the end of implementing an effective internal audit function; it is more like the beginning of a new year, and very similar to the approval of the organization's annual budget – where you have decided what the priorities are, what you are going to spend, where you plan to spend it and what you expect to get. But throughout the year you will still need to assess changes to the risk profiles and the related plan, propose adjustments to the audit committee, and most importantly, meet your many goals and objectives.

9.2 Interviewing Skills

Gathering information is a fundamental part of audit work as the auditor spends a great deal of time fact-finding. The starting place for establishing facts is simply to ask, and herein lies the importance of interviewing. Some of the synonyms for interviewing are:

audience, conference, consultation, dialogue, meeting, talk, examine, interrogate, question

We take a wider view of the concept and mean it simply to refer to 'talking with' in a structured manner. Dale Flesher has written that: 'The audit interview is a means of gathering facts, opinions,

and ideas, and therefore is an important source of audit evidence. It is a means of interpreting hard copy information . . . an auditor's skills in using the techniques of audit interviewing frequently determines whether he or she is perceived to be a professional'.[2]

The technique of interviewing should be mastered by the auditor and there is much material available on this topic that will contribute to this task. We see interviewing as a process, a task, a set structure, an audit standard and an exercise in understanding human behaviour. These components will be covered in the material below. Interviewing is based around effective communications and it is a good idea to remember the basic communications model to appreciate where things could go wrong and how communicating may be improved using Figure 9.2.

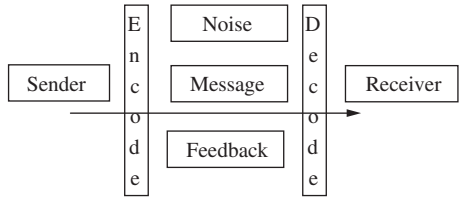


FIGURE 9.2 Communications.

The sender has to decide how to transmit the message which is then sent and decoded (rightly or wrongly) by the receiver. All this is against the background noise that consists of anything that gets in the way of clear messages being delivered and received. The positives are located in the feedback loop where understanding of the message is fed back to the giver to ensure it has been properly received and understood. Communicating is harder than it sounds and a quote from Madelyn Burley-Allen is apt: 'Speech is a joint game between the talker and the listener against the forces of confusion. Unless both make the effort inter-personal communication is impossible'.[3]

Types of Interviews

There are many different types of interviews that the auditor will undertake and within each type there may be several different categories. Most are founded on Kipling's six friends in terms of trying to find out *when, why*, *where, how, what, who*. One list of different types of interviews may appear as:

Initial contact with the client This interview may set the whole tone of the ensuing audit and determine whether the client perceives the audit as a positive constructive matter or a basic inconvenience. The terms of reference of the audit and management's particular concerns may be defined and a clear path made for the field auditors. This interview will probably be carried out by the audit manager and/or the lead auditor. One key feature will be an attempt to explain the concept of independence to management, whereby the auditor works on their behalf but with the best interests of the organization also firmly in mind. It is important that the promises made at this forum are followed up by the auditors who perform the work required. There is little point in having a highly skilled orator explain the audit objective, only to send trainees, who have a poor understanding of the important operational issues facing management, to perform the work. This initial contact is quite important, since some estimate that around 90% of people will decide what they think and feel about someone within the first 10–40 seconds of meeting them based on:

- Visual impact (what is seen) 55%
- Auditory impact (what is heard) 38%
- Content (what is said) 7%

Fact-finding These interviews may be seen as the backbone of most audit work and will continue throughout the course of the audit. It is essential that each such interview leaves an opening for the auditor to follow up the findings and revisit the interviewee if required. One must maintain a balance between 'getting the facts' and disrupting the client's work as these two forces will create some level of conflict. Negotiation skills and the ability to be firm, while at the same time remaining diplomatic, come to the fore. Some interviews will go well while others will be less successful and this point will have to be accepted by the auditor.

Corporate risk assessment survey A general assessment of the main operational areas in an attempt to define those with the highest levels of risk requires talks with senior management. These interviews allow the auditor to build in the organizational and managerial needs before formal plans are published. This type of interview is a chance to listen to high-level concerns as well as marketing the audit service to an extent. One such meeting at senior management level can raise the entire profile of the audit service immensely, if done properly. One may take this opportunity to 'sell' the audit product to managers who have had little or no contact with internal audit in the past.

Post-audit These potentially difficult interviews bring the main findings to the client's attention once the field work has been completed. If the client has been kept informed throughout the course of the audit then one may avoid confrontational closure meetings. Our reporting standards generally mean that we should not present management with surprises in the formal audit report. As such a type of negotiation process may arise where the auditor retains the main audit points, but tones down others where the client is able to bring a new perspective to the initial audit findings. Personality factors may create a form of barrier to the effectiveness of the audit closure process if we seek to establish a win/lose position with the client. Again the interview should be handled with skill and care if these potential traps are to be avoided.

Audit marketing It is possible to interview new and existing clients solely to convey the audit role as part of a marketing strategy. Audit services may be 'sold' to clients and one may enlighten managers on ways in which the wide-ranging audit role may be used to improve services and performance.

Recruitment Audit management may be asked to perform recruitment selection interviews and these are critical to the selection and appointment of suitable new audit staff. This is dealt with elsewhere in the training manual and at this stage it should be noted that appropriate skills should be acquired and employed by the appointments panel.

Staff appraisal As with recruitment interviews, staff appraisals are covered as a separate topic in the Handbook. Unfortunately, poor appraisal schemes and lack of interviewing skills tend to undermine the entire appraisal process and in so doing demotivate staff.

Fraud Fraud interviews should also be very carefully planned since they are covered by the Police and Criminal Evidence Act 1984. In addition to abiding by the rules, one is also charged with securing the necessary information that may contribute to the investigation. Skill is required in these matters and a limited amount of guidance is contained in the notes below.

Structuring Interviews

Interviews are structured meetings where information is provided and obtained. The interviewee must understand what information is required and the interviewer must likewise understand the information that is being provided. It is generally advisable to structure the interview since this tends to assist the task of exchanging information. The process should involve the following key steps:

Background preparation on the subject area Whatever the interview, it is always useful to do some background work related to the particular topic at hand. As a standard, one would expect the auditor at least to consider material that has been provided to the internal audit unit. This involves reviewing files, talking to auditors who have some relevant knowledge and obtaining any previous written communications with the party in question. It is extremely embarrassing to meet with an individual who refers to correspondence that was sent to internal audit in the past, which the auditor is unaware of. The audit information systems should be capable of isolating all records of past contact with managers, and sections of the organization. A suitable central database should be maintained by the audit administration officer who collects and indexes this information. The degree of preparation will be related to the importance of the interview. This may range from a basic internal search of the filing system (as indicated above) through to an extensive review of published material associated with the matters that will form the basis of the planned meeting. Most managers are greatly impressed by auditors who display some knowledge of the matters uppermost on management's mind.

Set convenient dates and times On the basis that an interview that is hurried with the constant pressure of other competing demands lowers the benefits that come from such a forum, it should be arranged properly. By this we mean that there should be sufficient notice given along with due regard for problems experienced by the client in finding the right time and place for the meeting. We obviously have to balance the need to complete our work promptly with the requirements of the client. Some leeway on our part is required if this balance is to be achieved.

Prepare checklist areas to cover This should entail a brief note of the areas that need to be covered as an *aide mémoire* and as a way of thinking through the information gathering process beforehand. It is possible to provide this checklist to the interviewee beforehand so that any preparations may be made that will expedite the process. As a rule, never list a series of detailed questions as this approach will come across as being far too mechanical in terms of reading the questions and repeating them in front of the interviewee. It also stops the auditor from using professional judgement to manage the interview process by changing the order and questions to fit the responses that are being provided by the interviewee.

Define objectives of the interview The next important stage is to state the precise objectives of the meeting. There are times when the auditor forgets the power of the audit right of access which forces managers to provide relevant information and explanation, as part of their managerial duties. This results in most requests from audit to attend an interview being readily accepted by managers who are aware of their special responsibilities in respect of auditor's requirements, which makes it easier to quickly convene meetings. There is nonetheless the danger that managers are present simply because of their desire to discharge their duty and not with any belief that they may benefit from such a discussion. The act of explaining the basis of the meeting should be designed to remove this psychological barrier and allow a free flow of information in both directions. If this is not done then the level of efficiency may decline as the interviewee responds rigidly, as would someone who is forced to furnish information.

Set the tone of the interview which should normally be open, friendly and positive The opening comments are commonly known as 'breaking the ice' and involve focusing on neutral topics such as the weather, so as to develop some form of immediate rapport. This is based to an extent on ritualistic behaviour that can indicate which social and political grouping each party belongs to, and set common standards of conduct. The point is made so as to provide a warning of some of the traps that the unwary auditor can fall into if this stage of the interview is overemphasized. To engage in idle social discussions can be very distracting for both sides to the meeting if this is not properly controlled. One might remark on general topics as a preamble to the real discussions but this should be contained as it will inevitably result in value judgements if too much depth is assumed. Seemingly harmless topics may hold a heavy political agenda; so, for example, a discussion on sporting events may end up in arguments about the relative attributes of cricket contrasted with football. The hidden agenda may be that one sport has a higher social status than the other (i.e. cricket is played by gentlemen). The conclusion then is that it is pointless becoming involved in discussing apparently neutral subjects as a way of setting the tone for an interview. It makes more sense to concentrate on the objectives in an informal manner and so avoid unnecessary complications.

Invite feedback on the audit objective and explain how the interview fits into the audit process It is one thing to state the audit objective and then break the ice with some opening remarks that show the human face of the auditor. Real progress occurs where the interviewee provides feedback by seeking further clarification where required. It is important that the auditor does not see this as a challenge to his/her position of independence but takes the view that all questions have a purpose and should be answered. If, for example, the client wishes to know why a different section with major operational problems has not been targeted for audit cover, this is a legitimate concern. The auditor must then provide a sensible answer and not just state that this is outside the terms of reference of the meeting. All legitimate questions from the interviewee should be addressed as best as possible, which is a guiding principle for positive points of contacts between auditor and interviewee.

Ask the questions and direct the interviewee to the key issues without restricting the responses The real hard work comes in the main part of the interview. We have set the client at ease and explained clearly the purpose of the interview. We have encouraged feedback and, where possible, have provided explanation. This sets the tone for a good meeting of minds with full and open discussion on real matters of interest to both sides. The time then comes to secure the required information in order to progress the audit objective and it is here that the interviewer must take the initiative and maintain this throughout the interview process. As with an orchestra conductor, we must merge into the background and let the interviewee talk but at the same time direct and control the proceedings. The interview will be based mainly on encouraging the interviewee to talk and this becomes the main consideration. Talking and controlling are two different concepts but there is a link; the person who does the most talking tends to be the one who controls the discussions. We must reverse this principle by the use of techniques such as prompting and recapping, which ensure the auditor is able to structure the discussions. We can only direct and control the interview if in the process we have listened very carefully to the client. In this way we will be able to fit what is being said onto the predetermined structure of the meeting. It is impossible to alter the course of a conversation in a natural manner, if we have not understood the point being made by the other party.

Run through matters dealt with during interview and clear up uncertainty It is frustrating to review interview records and pick out points that are unclear or ambiguous. These uncertainties

should be resolved at the time they are being discussed, that is, during the live interview. This can be at the time a point is being made where we can ask for further clarification, so long as this does not involve constant interruption. Where there are many inconsistencies, which would involve constant interjection from the interviewer, we may seek to summarize the points and so clarify these matters. There are some matters that are quite straightforward when first conveyed but clash with something that is said later, which is why it is so important to listen carefully to what is being said. We may diplomatically challenge points as they are being made, or review our notes and pick up these conflicts towards the end of the meeting. One needs to ensure that there is enough time to deal with the matters at hand and go through the notes at the end of the proceedings.

Conclude the interview with the usual courtesies We must retain a level of diplomacy at all times. Even where the interviewee has not been very forthcoming the auditor is expected to rise above this and remain polite to the last, which includes extending thanks at the end of the interview.

Ask for any questions There must be a clear stage at the end of the interview where the other party is allowed to reflect on what has been said and ask general questions. We have already said that all questions are asked for a reason and even where the auditor feels that they are immaterial, they nonetheless have to be responded to. Time should be allowed for this feedback and it should be encouraged. If, for example, the interviewee has no questions, we may give prompts by asking whether he/she is happy with certain of the points made, and in this way encourage a response. We do not want to leave a level of disquiet after the interview has ended.

Explain the next steps The last consideration is to explain clearly what will happen from here on. This should indicate the timing, who will be involved and how this fits into the overall audit process. The client is left in no doubt as to the value of the meeting and what may be reported by the interviewee to staff and other interested parties. It may be necessary to write to the interviewee and confirm points raised, although this can be a negative step that may lead to later disagreement on minor matters that detracts from the main concerns.

On the basis of much that we have already discussed, we may provide an outline illustration of how we might structure a typical audit interview in Figure 9.3.

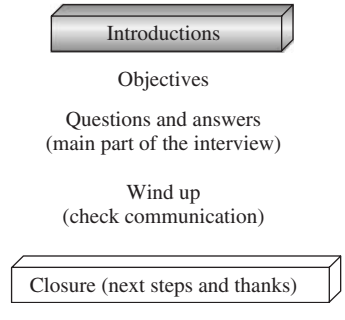


FIGURE 9.3 Interview structures.

Explanations follow:

- **Introductions.** This involves introducing all parties present at the interview and explaining their role and position within the information-gathering process.

- **Objectives.** What is hoped to be achieved from the interview is then fully communicated and further clarification provided if needs be.
- **Questions and answers.** The main body of the interview should then proceed in a way that flows naturally and promotes the achievement of the original objectives of the meeting.
- **Wind up.** The next stage is to recheck the information that has been given and any matters (such as the exchange of specific documents) that have already been agreed.
- **Closure.** An indication of next steps, further meetings and specific arrangements such as planned meetings with key staff should be given. Formal thanks (and possibly handshakes) should also be a feature of the last stage of the interview process.

Behavioural Aspects of Interviewing

What might appear a straightforward interview may go badly wrong and leave the auditor and client confused. There are many reasons that people act in an unpredictable way which generally stems from a lack of appreciation by the auditor of the behavioural aspects of audit work. The actions of one aggressive auditor who may have left many years ago may still be foremost in many managers' minds whenever the auditors call. There are many behavioural aspects that the auditor should bear in mind when conducting interviews and interviewees may possibly be asking themselves the following questions:

- What do they want from me?
- Are they human?
- Are they assessing me?
- Can I trust them?
- Should I tell them everything?
- What are they writing down?
- What about my problems?
- How can they help me?
- How will their work affect me?
- Who will be blamed if they find any errors?
- Are they going to propose drastic changes?

The auditor poses a threat in terms of the potential for making changes to the working lives of everyone they meet. People generally dislike change particularly where they cannot be sure how it will affect them. Where these changes are based on levels of unmitigated risk the auditor finds in the manager's area of responsibility, any suggested changes may be associated with negative connotations. These feelings can affect the way the interview progresses and the auditor needs to be sure that the audit objectives and how they should build into management's needs are carefully conveyed to the interviewee. The first few minutes of the interview may consist of a clear attempt by the auditor to explain the audit role and approach before a constructive dialogue may be entered into. It is also important to indicate the next steps that will be followed, after the interview is concluded. The auditor's actions must be consistent with his/her words and if he/she is seen as a spy for senior management, little or no cooperation will be received. The following records one difficult interview:

> A senior auditor arrived at an interview with the head of personnel (HoP) to discuss a planned systems audit of recruitment procedures. During a strained interview the HoP made constant

references to her files being available to audit at any time and she had nothing to hide. After a very difficult time, the auditor cut short the meeting and agreed to reconvene. The auditor later found that about a year ago, the HoP's files had been raided, in her presence, by a rather offensive audit manager (since left) during a fraud investigation and nothing was found. No reason for this raid was given, neither was an apology issued. At the next meeting with the HoP the senior auditor made reference to this raid. He dissociated himself from it, whereupon a more positive atmosphere reigned which resulted in progress being made on the audit.

The mismatch between what the auditor says he/she does and management's own understanding can lead to fundamental conceptual problems. This has to be fought against at all times by the auditor to dispel myths, and build proper working relationships. Even where the auditor is involved in investigations into irregularity, there is still a view that the auditor is primarily examining the circumstances at issue and not the people concerned. Where a name can be fitted to a problem, this should be a natural consequence of the proceedings and not a witch-hunt. One of the hardest challenges in the audit role is seeking to reconcile the assurance and consulting roles. We would hope that the image of the jackbooted 'find the transgressor' auditor does not cross over into our main role in assurance auditing and make constructive communications with management and staff impossible. Much resistance from client can be pre-empted by discussions on this point in a frank and open manner, so long as our actions coincide with our words.

Non-verbal Communication

Non-verbal communication gives clues as to how each party to an interview really feels. We cannot say to an interviewee that we have plenty of time to discuss issues while continually checking the time and tapping the desk with a pencil. Examples of non-verbal communication include:

General body movement People who move around a lot are generally very busy or have nervous energy. Some people will move more when they become agitated and under pressure to make some form of decision, while others are more relaxed and give an air of command over the situation. There is not much that can be read into this as a nervous person may generate much work, while a laid back person may generate good control over a potentially chaotic situation. Medical conditions may mean the person cannot sit in one place for long, or appears to be hesitant in physical movements. Overactive thyroid glands can lead to a heightened state of readiness that may make the person appear to be overanxious, or overactive. The main point is that one must allow for many imponderables and not arrive at value judgements based on the way a person's body responds to the environment.

Eye contact This can be used to develop a working relationship with the interviewee. It is an oversimplification to suggest that people who cannot make eye contact have something to hide, as this ignores many other possibilities such as cultural bias and general tendencies to look elsewhere. The point about eye contact is more relevant to the auditor in reviewing their own behaviour. To this end it is generally advisable to make regular eye contact with the interviewee as this does tend to convey a feeling of openness and sincerity. At the same time excessive contact may be deemed intimidating or, on the other hand, being excessively intimate, may again be deemed as a possible threat.

Physical position and posture The way the chairs are arranged in an interview room can impact on the proceedings and imply either a formal event or a less ceremonial atmosphere. Sometimes basic practical points come into play where there is no space for the interviewee to lay out working papers as this act is deemed to be the province of the auditor alone. One large chair behind a desk faced by a smaller one for the interviewee can represent the social (or working) status of the two sides to the discussions. Leaving a third person physically to one side and removed from the main proceedings can indicate that this person has less to contribute and is so isolated. Leaning back indicates boredom, withdrawal or an invitation to the other party to assume the initiative. It can also suggest that the person is in control and does not have to impose a greater physical presence on the proceedings. Leaning forward can be contrasted with this as it implies attentiveness or some anxiety. Words and actions should coincide; for example if a client says, 'Can I tell you something in confidence?', the auditor could reinforce a co-operative stance by both leaning forward and refraining from taking notes. Much of this comes naturally and contributes to a smooth flow of information.

Touching This feature can be both positive and detrimental depending on how it is used. Firm handshakes tend to support a good working relationship, while a hand placed on the shoulder of someone sitting down can be patronizing or even intimidating. Different cultures make varying use of intimate gestures such as hugging or kissing the cheek. The best approach is to assume the least offensive position, which translates to minimal contact if in any doubt.

Hand movement and facial expression Gesticulating with the hands is one way of getting points across and is used in most cultures where hand actions coincide with what is being said. The hand along with the face gives visual clues as to what is being said and the stress that is given to different parts of the presentation. Open hands tend to represent honesty and a drawing in, while chopping hands indicate a level of physical aggression that can be worrying if done excessively or at inappropriate moments. The auditor should watch for these clues and the idea will be to probe areas that are obviously stressed as being of concern to the interviewee.

Silences This can be used as an effective tool during an interview. Most people dislike silence as this creates a vacuum that they have no control over. It also focuses attention on the party that is most uncomfortable. Sometimes we may get more information on a sensitive issue by simply remaining silent as the interviewee gives guarded responses that are punctuated with constant pauses. Silences can be interpreted in many ways. They can imply that we are not satisfied with the answer and want it rephrased or that the meeting is overheating and both sides need time to reposition. If the auditor says, 'Tell me about your role?' and then sits backs in silence with pen and clipboard in hand, this may signal an important part of the interview where all is revealed. Further silences may be used to suggest that there is more to offer and encourage the interviewee to go into greater detail. Silence also underpins listening skills as one can only really take in material where the ears are in use and the mouth is resting. Silence should never be used to intimidate or manipulate the client as this will be seen as a bullying tactic that has no place in the audit role.

Where the words spoken do not match other signals then the other party may not believe the representations and may be more willing to rely on the latter to guide them. Auditors need to check their own actions and also be sensitive to signals received from the interviewee. This is particularly relevant where certain issues need to be probed more deeply by the auditor. By the same token one should not attempt to manipulate the interviewee through an obsessive study of body talk. There is a view that we need to inject some degree of conflict into our role as auditors

as this tends to support change programmes, in contrast to a cosy relationship where the status quo is maintained at all costs. Controlled aggression, annoyance and the considered use of some emotion may be seen as part of the process of challenging management to take up and resolve significant risk. This approach can be used as a lead to 'getting things done'. However, it can have obvious disadvantages as it is based mainly on quick judgements by the auditor that do not really fit into the professional audit role. Nonetheless, it does have a place particularly where dealing with people who can operate on a high stress plane (normally top management). Securing action at this level may require a less conservative mode by developing a more confrontational type environment, and non-verbal communication is a supportive device. The CAE should be involved in any decision to promote this position.

Types of Questions

Some interviews go on for hours while others last a few moments and these two extremes do not necessarily coincide with the auditor obtaining full or limited information. The success of an interview is not only measured by length of time. Long discussions may be constructive but can result in inefficient use of time. The efficiency of interviews increases by the selective use of different types of questions. Interviewees are guided by skilful use of questioning so that material issues are expanded on while specifics are dealt with more quickly. Types of questions include:

- ***Open questions*** such as 'Tell me about your job'. There are times during an interview when we wish to give the interviewee a free hand in discussing a particular issue. It can open up a flood of material that can become uncontrollable if it is not structured at all, and in this way it should be used only where appropriate. It is best to set a scene by describing a set of circumstances and then ask the interviewee to comment on this. The answers can be structured to an extent by asking closed questions as the discussions progress, although this may involve an amount of interruption. The technique tends to stimulate a positive atmosphere on the basis that most people like to talk about their work area. If the answers become too long, or go in different directions, we may gently interrupt the proceedings by deferring specific matters for later coverage. The topics that we deal with using open questions must be related to matters that the interviewee has direct knowledge of, so that a value-based opinion is not provided that delves not on facts but into pure conjecture. So we can ask questions like 'Tell me about your latest strategic goals', but not value questions such as 'Give me your views on whether the organization treats people fairly'.
- ***Closed questions*** such as 'Do you work in the accounts department?' This requires a basic yes/no answer that can be recorded straight away. This is a useful way of getting precise responses to important factual questions that does not rely on judgemental material or long-drawn-out discussions. Name, post designation, start date and specific factual matters can be dealt with in this forum. Having said this, the extensive use of closed questions will elicit very limited information and can turn into an interrogation. It will also create a potentially confrontational mode as the interviewee is subject to a barrage of closed questions that result in the provision of substantial amounts of basic facts. It is best to use closed questions sparingly perhaps at the start of the interview and whenever we need basic detail, or need to check what has been said earlier. In general they should be avoided if we wish to develop a closer relationship and understand the real issues facing management.
- ***Probing questions*** such as 'Tell me more about xyz'. These types of questions are used where the client starts a discussion but does not go into sufficient detail. Points raised by the interviewee can be highlighted and further details requested, as a way of directing the

discussions. This requires an amount of recapping, which makes the interview process longer and slightly less smooth. However, it means that we get a complete picture of items important to the audit objectives. The problem arises where the auditor probes certain areas that the client is not comfortable with. Some people purposely avoid issues that they feel can leave them open to criticism. In this environment the auditor may find a reluctance to address these particular topics even where there is some probing. Rephrasing the question is another way of returning to a defined topic as will reviewing what has been said. Ultimately it is difficult to get someone to talk about a topic that they wish to avoid without injecting some conflict into the occasion. It is here that interview skills should come to the fore through a mixture of gentle persuasion and firm perseverance. There is a need to achieve a fine balance between the auditor's right to information and explanations while recognizing that we cannot really force people to talk openly.

- ***Confirmatory questions*** such as 'Your job description refers to an xyz, is this correct?' Compliance auditing recognizes the realities of business life and the fact that not everything is always as it should be. Furthermore there are times when we need to double-check an assumption or official position as a way of getting to the truth. It is within this context that we will seek to confirm our understanding of events, systems, processes, circumstances and whatever else we have to research in the course of our work. The ability to recheck matters in a factual manner without causing offence is useful where we need to obtain reliable information. Again we need to avoid the interrogation stance which is why the use of this approach should really be restricted.
- ***Clarification*** along the lines, 'I thought you said that you worked for Mr X?', when the interviewee has just contradicted himself. We are fast moving into the territory of manipulation where the auditor tries to squeeze otherwise classified information from a third party. Where there is an obvious inconsistency between the detail that is being provided it is best to place this problem directly in front of the interviewee and seek an explanation. There may be a straightforward reason for this and the opportunity to explain should always be provided. Where there is not, we will still need to obtain clarification as our record of the meeting will not be acceptable, if gaps and conflicts remained unresolved. Again the most efficient method of solving these 'mysteries' is simply to ask.

In general, one should not use the following types of questions:

- **Leading questions** such as 'Surely you check these invoices before approving them?' This category of question encourages a predefined response that has been invited or hinted at, while the interviewee tends to feel obliged to provide the acceptable answer. The problem is that it does not fit with the search for the truth, which is the main aim of the interview. In this way we can more or less ban the use of leading questions as a generally acceptable practice.
- **Loaded questions** such as 'You appear to be more qualified than your boss'. This incorporates a degree of emotion by being directed at a 'soft spot'. Some may feel that it will get the other party on the side of the auditor by implying a position that sides with them in favour of another outside party. Playing politics has no place in audit policy, not in terms of its usefulness but more in terms of the danger that comes with not saying what you mean or meaning what you say. Audit policy should rule loaded questions generally out of bounds.
- **Trick questions** along the lines, 'You say that you have worked here for three and a half years; what date did you start?' The auditor may appear to be clever by playing a game of 'one-up-manship'. This involves keeping one step ahead in terms of general knowledge and usually hiding certain pieces of information so as to rely on this extra insight for use at a later

stage. There are many implications of taking a stance along these lines which have no place in the audit role. As with the other approaches there is little point in retaining the use of trick questions as part of audit standards on interviewing.

One principle that should be applied is that constant feedback should be obtained throughout the interview and matters double-checked as far as possible. For more formal occasions the interviewee should be asked to comment on the documented interview record at the close of the meeting.

Conduct during an Interview

Auditors carry out interviews many times and tend to acquire the necessary skills as their level of experience increases. There are several points regarding how audit interviews are conducted that should be noted:

1. The interview should be planned. The tendency to rush headfirst into interviews should be dealt with by ensuring that the concept of defining a plan within which the interview will fall should be part of the conduct expected by audit management from their staff.
2. Auditors should familiarize themselves with the area under review and risk register that is in use. It is a necessary part of the preparation process and helps raise the auditor's credibility. It also means that answers can be understood and evaluated much more readily.
3. A structure should be aimed at so that there is introduction, fact-finding and winding-up. This involves formal introductions, getting the required information and explaining what happens next.
4. Observe the requirements of the auditor's code of conduct. Superimposed over the detailed code of conduct covering interviews, we have the general auditor code of conduct that also covers the way auditors interface with others during the course of their work. Basic rules on politeness, diplomacy and offensive behaviour should be firmly in place and apply to the interview situation as well as other points of contact with colleagues, clients, and members of the public.
5. Break the ice when starting the interview since a formal mode once entered into will probably be maintained throughout the interview. We would expect auditors to assume a working relationship with people they deal with in an interview situation. The world of internal auditing is becoming aware that the key to professional auditing lies in effective communication skills. Clearly, there is little room left for the auditor who is unable to develop the personal presentation skills so necessary to the art of successful communication. The days where the cold, obnoxious auditor, who is disliked by all he meets, is allowed to remain in employment are fast coming to an end.
6. Formally conclude the interview and do not leave any unresolved matters. Very often people meet, agree on many things, and then depart without achieving anything in real terms. Many months later all that has been promised falls into a blurred memory with the passing of time. We expect auditors to avoid this unsatisfactory position by requiring them to tie up loose ends and to ensure there is a proper conclusion to all that has been formally agreed on.
7. Try to avoid making statements or giving opinions since although they might make the interview more interesting, they may be perceived as formal audit comment. They also tend to be based on an incomplete picture of the areas under review. Jumping to conclusions

and/or providing the solve-all answers to complicated problems that have not been researched to any extent is a basic flaw exhibited by most new auditors. To allow such behaviour is unfair to the client, who cannot be sure whether a formal audit opinion is being given. It is also unfair to the auditor who assumes a know-it-all stance that defeats the audit objective in that conclusions are drawn without any supportive evidence or proper research. Fortunately, as we have suggested, this defect is found mainly in people new to the audit arena and not the more experienced audit professional.

8. Formulate specific objectives for the interview. Meetings and interviews are often held as a way of getting to know people who may have been mainly dealt with over the telephone or via e-mails. These face-to-face discussions may not have any real purpose as hours go by and an assortment of unrelated issues are chewed over by both sides to the conversation. To avoid this loss of time, we must set clear objectives for the interview and ensure that the checklist of areas to cover (drafted beforehand) reflects this objective. It is surprising how often an interview is brought back into focus by the technique of referring back to the original objectives, so that unrelated points can be sidelined before the direction of the discussions changes permanently.
9. Use negotiation skills where necessary. This means that one defines points that may be given up and those that have to be preserved beforehand so that some flexibility can be assumed during the interview. A win/win position encourages each side to get something from the event and this can only be good in terms of its impact (perhaps we can call this a 'feel-good factor'). Giving ground is one way of arriving at this position and as such should be built into the code of conduct for interviews. The converse, where the auditor stands his/her ground in a rigid manner, oblivious to all that is being said, generates the opposite effect. This again can be addressed in a suitable code by making this approach generally unacceptable.
10. Ensure that audit brochures are available for the interviewee. It is important that the definitions and details that appear in any brochure and website material coincide with explanations provided during the interview. It is bad practice to force brochures on persons we come into contact with, as this engenders a feeling of 'hard sell'. Where it is appropriate, in that there is a request for further information expressed during an interview, a suitable brochure will provide a positive response without going into too many details that detract from the real aims of the meeting. It also means that material put in front of the other party will have been carefully considered and planned by senior audit management.
11. One should list all the items that are not immediately available but have been requested by the auditor and this list should be checked at the end of the interview. This device saves time in the long run as it ensures a complete list of outstanding material.
12. Explain the purpose of note-taking and ensure that the notes reflect the information received. It is simply good manners to explain why one is writing all that is being said in an environment where this may not be the accepted norm.
13. Watch the human relations aspects and body movement. A suitable code of conduct will not allow the auditor to continue an interview where the other party is obviously distressed.

Above all listen, listen and listen. It is hard to set a standard on this but we must demand that our auditors have mastered the fundamental skill of being able to concentrate not on what they are saying (or plan to say) but more importantly on what is being said to them. The significance is such that if audit management is not able to train its staff in this skill, then these staff should be released and new people recruited.

Barriers to Good Interviews

Much can go wrong with an audit interview:

- Guarded responses from the interviewee can give incomplete information. This may occur where there is mistrust between auditor and client. Explaining the purpose of the interview along with the use of open questions can help shift the interviewee's position. Probing questions can help so long as a working relationship has been established which allows the free flow of information between the two sides. A guarded response may create a reaction from the auditor that leads to a confrontation as the auditor becomes more insistent that all questions are fully answered. This elicits a greater defence from the interviewee and we approach the stage where the interview breaks down. The correct approach is to seek to understand why the interviewee is worried about giving complete information. We may then break down this barrier by explanation and probe points that need to be explored.
- Poor timing can result in the interviewee being too busy to spend much time on each audit question. Most managers try to squeeze an interview into a busy work schedule and this can interfere with the free flow of information. The real-life practicalities of the working environment make this a norm rather than an exception that must be appreciated by the auditor. The key here is to base the discussions on the benefits that accrue from the interview, which in the main will be associated with an audit. Managers will assign time to matters that fit with their objectives and provide defined benefits for them. The fact that it is management who is responsible for installing and maintaining systems of internal control to tackle risk can be used to stress the need for audit cover. It will help generate the view that time spent assisting audit in this matter provides good VFM. The auditor does not have to 'sell' the audit service by the use of gimmicks and free gifts, but there is nonetheless a need to achieve support from management and the organization generally. Actions must fit in with representations and the auditor cannot explain the importance of management spending time in audit interviews while engaging in idle conversation during these meetings. To this end, the structure of the interview and the way it is managed should be designed to ensure it is an efficient use of time (for both sides). The onus is on audit to manage the time properly where the interview has been convened at the request of internal audit.
- Defensiveness can result where the auditor poses a threat. A guarded response means that the client provides information that is politically acceptable while not necessarily addressing all relevant matters. Defensiveness is more proactive in that the interviewee will purposely seek to protect their position in the face of a perceived threat from the auditor. We have discussed the potential conflict between systems work and special investigations and this makes it difficult to reconcile the two approaches of policeman/advisor. This conflict can interfere with the interview process where the audit's power to initiate proceedings that could end up with an officer being dismissed does not allow a free flow of views. The worst case arises where the manager feels that audit is hiding behind the systems audit cover to disguise the fact that they are actually investigating the manager. A study of the behavioural aspect of auditing that was discussed earlier will assist the auditor in managing this situation.
- Personality clashes spoil the whole interview process. The first few seconds of contact between two people are crucial in that they will make fundamental conclusions about each other. These conclusions will be set and whatever happens next will be interpreted within the framework of these initial views. Some suggest that the chemistry of interaction between two individuals has an unknown quality. A further barrier to good interviews is a clash of personality where a win/lose position is assumed by both sides. The actual matters for discussion fall into the

background against this 'battle of minds' that is a feature of this type of situation. Auditors are bound by a strict code of conduct that bans them from engaging in heated argument and accusation and this is the first principle that should be applied. There is obviously the usual standard where we would seek to assume a working relationship and concentrate on the issues at hand and this must be explored as a possible solution. In the final analysis where there is an unresolvable clash of views with no logical basis, the auditor will have to withdraw from the interview and seek another way of getting the required information. This may be done by a more senior auditor, or through correspondence. If the interviewee fails to cooperate despite all efforts from internal audit then we would seek to have the matter resolved at a higher level. We can accept a personality clash with one particular auditor but not a general inability of a client to respond to legitimate audit enquiries.

- If the auditor insists on jumping to conclusions, this may turn the meeting into a farce. If we turn the interview into a 'who knows best?' battle, then little constructive work will be completed. These snap evaluations are sometimes made by an auditor as a short cut to doing the necessary detailed audit work, which may destroy the credibility of the entire audit process. The auditor is there to secure relevant information and after having completed the necessary research, will furnish a suitable audit report. A know-it-all attitude by the auditor can also lower the quality of the interview. Here the auditor should realize that they can never know as much as the manager who actually runs the area under review. This task is easier if auditors remember that they are experts in control not operations. It is not the auditor's duty to second-guess management or show that audit knows more than managers about a particular work area. It is up to audit management to stop auditors who exhibit this disturbing trait.
- Poor listening by the auditor will frustrate the interviewee. The client will sense lapses by the auditor particularly where the questions show a misunderstanding of what has been said earlier. It is a precise skill to alter the tone, content, and order of questions in line with information that is steadily provided during an interview. This skill depends wholly on the auditor having listened very carefully to the other party so that the required adjustments may be made as the interview progresses. Where the auditor is unable to take a back seat and listen, this proactive approach to information gathering will be impaired. One way of promoting good listening is to seek clarification and test understanding of what has been said. Remember people can listen and still be in charge of the interview. It is important to employ dynamic listening with positive reinforcement and a conscious effort made to understand the messages being provided.
- A general air of mistrust can result in constant checking and rechecking by the auditor and the conversation may eventually deteriorate. We have suggested that the auditor seeks confirmation of what has been said without using 'trick questions'. This is the correct approach but can become annoying if handled badly. Going over notes and rechecking everything can give the client the impression that they are not trusted by the auditor. It can be perceived as a trick question in that it may appear as if the auditor is looking for inconsistencies or encouraging the interviewee to change his/her mind as if the truth was not given earlier. Much is a matter of diplomacy and tact. The auditor can defeat this potential barrier by making it clear at the outset (along with explanation) that this device of rechecking what has been said will be applied.
- Polarization may appear where the two parties take firm opposing views and place all issues within this narrow criterion of right or wrong. Working relationships may break down where this persists. Personality clashes result in differences that have no logical basis, while legitimate differences in opinion occur often without creating any real difficulty for the parties involved. In fact, a healthy debate can result where we impart an honest belief in our position, say, in respect of the importance of good controls. The barrier arises where we cannot accept that there are different views that can each be respected. A 'childish state' makes a view right or

wrong, and the person giving the view right or wrong (i.e. good or bad). Where this position is entrenched, we arrive at polarization where everything the other party supports is classified as wrong. Without going into detail the simple solution to this is to assume a mature position (in contrast to childish) and ensure that all discussions are made on this level.

- A poor reputation by auditors may lead the interviewee to take a flippant view of the audit process. The auditor is both a person and a representative of internal audit. Anything said or reported by internal audit has been done so in the name of the CAE. We cannot argue that an earlier encounter with an unprofessional auditor has nothing to do with us. We can overcome the poor reputation by an approach that is obviously based on high professional standards of work and objectivity.
- Information overload results in one or both parties being unable to keep up with the information exchange and if the auditor does not own up and seek clarification much detail will be missed. Technical jargon is generally used to mislead. In practice, all matters can be conveyed in an understandable form as long as each party has been open and appreciates each other's level of knowledge on the subject discussed. Everything cannot be covered during one meeting particularly where the interviewee insists on going into great levels of detail. As such, a common-sense approach must be assumed where general matters are dealt with first and specifics left for another occasion when the auditor has more knowledge of the systems under review. The other side of the coin is where the auditor is giving details of the audit performed and there is only so much detail that can be digested at any one session. Oral presentations using visual aids and handouts may replace the formal interview forum where it is important that complicated concepts are conveyed and understood. Most people switch off where great masses of data are thrown at them with no structure or order. These matters should be addressed before the interview is set up.
- Noise occurs where external factors interfere with communication and this ranges from distorted perceptions through to low-flying aircraft. There are many times when it is best to remove someone from their work area to an environment that is controlled to ensure the effective exchange of information. The main disadvantage is the lack of ready access to relevant files and systems for demonstration purposes. This is along with the danger in removing the auditor from the work environment that may give many clues to control issues. One solution is to do an initial meeting away from the office and later more detailed discussions at the workplace. Much depends on the objectives of the interview.
- Unclear ideas lead to confusing thoughts being conveyed and this will be difficult for the recipient to digest. This occurs where, for example, the auditor has a poor grasp of the issues that management face or feel it is his/her duty to superimpose on management an artificial audit view that has not been well thought out. Since the interview involves an exchange of information based around a structured series of questions, there is a need for common ground through which such a process should operate. Where this common ground is impaired by obscure ideas there will be a weaker structure through which the exchange of information can occur. Unclear ideas usually result from the auditor assuming an understanding that is not really there. It arises from a false sense of higher knowledge that the person in question feels he/she should possess. There is no real answer to this problem outside the need to base one's views on professional, well-researched audit work. Honesty is another important consideration based on the fact that there is nothing wrong with making it clear that the auditor has a limited amount of knowledge on the topic under consideration. Honesty also appears where the auditor admits that he/she cannot solve all problems that confront management. Bearing this in mind, the auditor may convene a useful discussion where each side has a clear understanding of the knowledge base of the other.

- Language problems may arise where accents, terminology and speech patterns interfere with the information exchange. Constant feedback will be required to clarify any uncertainty. It is also the case that one quickly becomes used to accents as the conversation progresses. Tact and diplomacy should be fully applied in this situation along with a level of openness in explaining any difficulties, rather than a pretence of understanding with a view to saving embarrassment. Where language is a real problem, the process of assigning a suitable auditor to the project should include a consideration of these concerns. It may also be wise to send two auditors to the interview on the basis that a joint effort in interpreting the interviewee may bring better rewards.
- The auditor's perceptions and own personal bias may distort an interview. This is very dangerous ground and the auditor's independence, which is the cornerstone of the audit function, depends on objectivity of mind. It is only the professional auditor who can recognize and then rise above their personal views and bias, with a view to discharging the audit objective.
- Where an interview is obviously not working, it is generally better to cut short the meeting before it actually breaks down, and think of adopting a new strategy to secure the necessary information.

Dealing with Difficult People

The auditor should be equipped with techniques to deal with difficult interview situations. There are different approaches for different situations and, for example, if someone is excesively talkative it may be necessary to interrupt occasionally. If the respondent is unhappy with the interview then it may be an idea to explore the reasons. A quiet person may be shy or bored, and it may be possible to introduce the subject being discussed in a way that is meaningful and which fits the value system of the individual in question. It is important to assess the visible aspects of a person in terms of their appearance, behaviour and what they are saying. Underneath this visible part of the 'iceberg' may be a whole range of hidden aspects based on the person's motives, value systems, and whether they see the interview as having a potentially positive impact on their position. There is guidance available on managing conflict and extracts from one reference by Gene H. Johnson, Tom Means and Joe Pullis follow:

> Several 'people principles' can guide the auditor in this aspect of negotiation:
>
> - Separate the individual from the context of the conflict.
> - Consider the opposition's view of the conflict.
> - Involve the opposition in the decision-making process.
> - Discuss emotions openly.
> - Communicate, communicate, communicate.
>
> Auditors should insist on using objective criteria as a basis for any solution . . . When establishing criteria, auditors should:
>
> 1. Step away from the conflict and objectively consider what might be appropriate criteria.
> 2. Think through their perceptions and be open to the reasoning of others.
> 3. Never yield to pressure or to an unjustified 'company policy'.
>
> . . . Conflict is an inevitable part of the auditor's work life. It can either be managed to move the organization forward, or it can make everyone miserable. Auditors who can negotiate with

others in an effective, harmonious manner will improve the chances that their recommended changes will be truly effective.[4]

Standardized Procedures

IIA standards require the CAE to establish written policies and procedures to direct the auditor's work and the audit manual should include a section on interview procedures. These procedures should cover the following areas:

1. The level of preparation required and the type of matters that should be considered before the interview is held. A standardized checklist may be used to cover most of the key areas, bearing in mind that many items may not be applicable, depending on the type of interview that is being dealt with. Some people do not like preparing for interviews because they like the spontaneity of just turning up, or they just do not realize how important it is to make preparations. The standardized checklist helps overcome these problems.
2. The way audit objectives are established for the interview. These should be formally set as a way of maintaining a clear direction over the process and not wasting time. The extent to which these objectives have been achieved may be documented after the event as part of auditing standards.
3. The various forms that should be used to document the interview. These will record the information that has been provided and also allows a review by the audit manager at a later date.
4. The way notes are maintained and checked with the interviewee before the meeting is concluded. Setting this process as a standard makes it a requirement to ensure that the notes are a fair representation of what has been said.
5. The fact that summarizes of the interview should be included so that one need not re-read the entire record to appreciate the main issues. A front sheet may provide a summary of the interview that lists the key points and the implications of the representations that have been made. This acts as a major convenience, particularly where the interview has taken a long time and covered much ground.
6. The way that representations should be verified by the auditor. We should seek to set standards on ways that information can be checked before it is deemed reportable. One useful technique is to secure copies of key documents that have been referred to by the interviewee. For example, if we have been told by a manager that he sent a memorandum to staff instructing them not to install unofficial software onto their computers, we may ask for a copy of this document. This will then be attached to the interview record.
7. The way that outstanding documents referred to during the interview may be followed up. We would have to establish a standard on following up matters that had been promised during an interview and the review process should include a consideration of outstanding items.
8. Procedures for ensuring that excessive time is not spent in interviews. Even where we are in direct discussions with officers and others, this is not necessarily a good use of audit time. It still has to be justified as time charged to the job in hand. Procedures should require the auditor 'to ensure that all interviews constitute an efficient use of time and contribute directly to the achievement of audit objectives'. This would then be a consideration during the review process.
9. The way interview notes are reviewed by audit management. Any checklist for reviewing audit files should include the interview record. The usual problem is either there are no records

of interviews with officers or there is a rough note that is very difficult to decipher after the event. Some auditors go to the other extreme and spend hours typing their notes when a carefully made hand-written record on standardized documentation would have sufficed.

10. The way facts obtained in interviews are quoted in audit reports. Audit standards should cover this point so that any mention made of matters obtained from an interview is properly presented. Reporting devices such as 'management has indicated that . . . ', or 'we were advised that . . . ', or 'the figure quoted by management is . . . although we have not been able to verify this in any way . . . '. We must make an accurate account of the status of information that may be derived from a passing comment by a manager. This contrasts with a formal audit testing process from independently confirmed sources.
11. The way adverse reactions from the auditee may be dealt with. We have mentioned the possibility of a breakdown in relationships and here we suggest that formal standards should be in place to cater for auditor conduct where proceedings may otherwise become heated.
12. How to deal with an interviewee who appears to be withholding information or refuses to provide vital material. The auditor will probe, diplomatically repeat requests and restate any concerns about a lack of information forthcoming from the interviewee. Where these devices fail then standards will indicate next steps that should include referral to audit management, specific written requests, complaints to the interviewee's line manager and so on. The auditor will be expected to follow whatever has been established as the prescribed procedure in this case.

There should be clear policies on audit protocol covering the way auditors explain their role and conduct themselves. This should start with the wide privileges granted to the auditor and the need to avoid abusing this. These rules must apply even where the client adopts a less diplomatic stance. Furthermore, a formal complaints procedure should be installed to pick up any problems resulting from the interview process.

Recording the Interview

It is good practice to record all interviews as part of auditing standards. What at first may seem to be bureaucracy in its purest sense does have an underlying reason so long as there are rules based on the sensible application of this requirement. Some of these rules are:

1. Apply different standards to different types of interviews. Some may be limited notes on key points on one sheet of paper. Other more formal interviews may be fully recorded verbatim. It will depend on the circumstances, although we should expect some form of record for all interviews.
2. Ensure that signatures applied are appropriate to the circumstances. Again this will depend on the circumstances as formal interviews may be fully signed and witnessed (e.g. fraud investigations) while others may not be signed by the interviewee but simply checked for accuracy then filed.
3. Provide a front summary sheet that contains objectives, results and conclusions that can be reviewed by the audit manager.
4. Use standardized documentation for all interview records. Remember different interviews will require different standards and we should have a batch of each type in our possession.
5. Type the record where necessary while retaining the original. This applies to formal interviews that may end up in court or at a disciplinary hearing or a forum involving an external review.
6. Retain documents referred to in the interviews with the record cross-referenced to the point where they are introduced by the interviewee.

7. Apply the usual standards of place, date, time, people present, audit job and reviewed by. Page numbering, e.g. page 1 of 5, 2 of 5, etc., ensures that documents are complete. It should be clear (from initials placed in the margin) exactly who said what during the interview.
8. Re-read notes for consistency. We can apply the 'six months later rule' and ensure that the record is understandable in six months when the interviewing auditor may have left.

Interviewing is widely used to secure audit information. Interviews intrude into the interviewee's world and may be resisted or encouraged depending on the relationship established. Experienced auditors set up interviews and secure information in an efficient and effective manner. The interview is a two-way process and the auditor must convey audit objectives clearly and convincingly. There are many barriers to good interviews and these should be recognized and carefully managed with the aid of a comprehensive audit manual and training workshops.

9.3 Ascertaining the System

Systems-based auditing relies on evaluating the whole system of risk management and internal control, which ensures operational objectives will be achieved. This task can only be performed where the systems that are being considered are properly understood, which in turn relies on the auditor's ability to document the system efficiently. There are several alternative methods, each with its own advantages. Some of the more popular ones are mentioned here.

Alternative Methods

The main options that the auditor has for documenting the system are:

1. narrative notes
2. block diagrams
3. flowcharts
4. internal control questionnaire (ICQ).

There are different types of flowcharts which are shown in Figure 9.4.

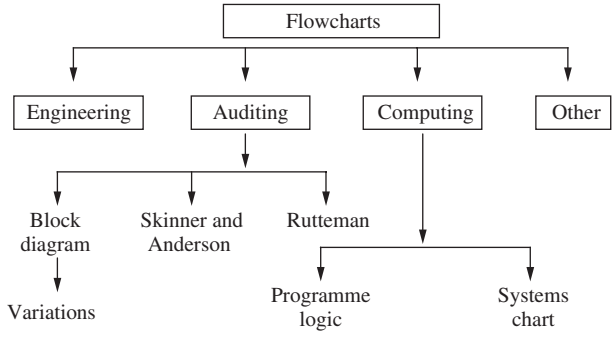


FIGURE 9.4 Types of flowcharts.

Despite clear differences between types of flowcharts, there are basic principles per Figure 9.5.

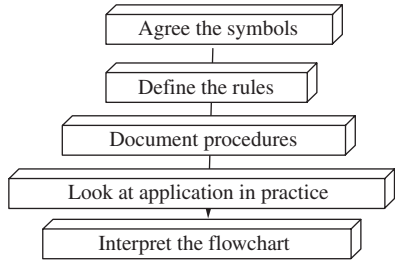


FIGURE 9.5 Basic flowcharting rules.

Securing the Required Information

Before the auditor can 'capture' the system, information must be secured through fact-finding. The auditor should interview the line manager and operatives to elicit a picture of operations. Line managers will have an overview of what goes on in their areas of responsibility and this is the starting place for the full audit. It is only when the operatives are seen that a truer picture is obtained as answers highlight non-compliance and/or poor controls. The auditor decides how far to follow the system if it links into other systems. This is clear from the defined scope of the audit in the assignment plan. New information that extends the systems boundaries is brought back to the audit manager for further consideration. When the system is being written up, gaps in acquired information may require further investigation. Armed with predefined checklists the auditor should direct interviews to cover all important areas. Capturing the flow of documentation and information should be key concerns. The auditor should try to document the system and consider whether it equates to the 'official system'. Different versions of the same system may result from misunderstanding by operational staff and this should be seen as a finding in its own right. Walk-through testing means that the auditor will point to examples as the system is explained by the client to help illustrate underlying processes. The information-gathering process may bring out weaknesses which might be discovered by the auditor or expressed by the interviewee. This aids the auditor in evaluation, and it is not necessary to keep ascertainment and evaluation separate. It is dangerous for the auditor to jump to conclusions and start recommending action at the ascertainment stage no matter how impressive this might appear during initial interviews.

Narrative

Systems are set out by straightforward narrative where the main parts of the system are noted in point format. The processes are described from start to finish to convey the required information on which to base an evaluation. The bulk of these systems notes may be taken direct from the interview with the operations manager. For simple systems that do not involve much document flows, this may be sufficient. For more complicated systems it may be necessary to go on to draft a block diagram and/or a detailed flowchart. Narrative provides a useful short-cut to systems documentation and as long as it conveys the right information clearly, it is a valid technique. It should be possible to cross-reference relevant documents to the narrative and then attach them to the notes for future use. Structured narrative notes divide the operation into sections or people alongside brief notes on each activity to form a diagrammatic representation of events. This might appear as Table 9.1.

TABLE 9.1 Structured systems narrative notes.

System stage	*Department A*	*Department B*	*Department C*
1	notes xxx	notes xxx	notes xxx
2	notes xxx	notes xxx	notes xxx
3	notes xxx	notes xxx	notes xxx
4	notes xxx	notes xxx	notes xxx
etc.			

This captures the system simply on a single document without needing detailed symbols and keys.

Block Diagrams

Block diagrams fall in between detailed flowcharts and narrative. They consist of a series of boxes each representing an operation or control. It provides a simple diagrammatic representation in Figure 9.6.

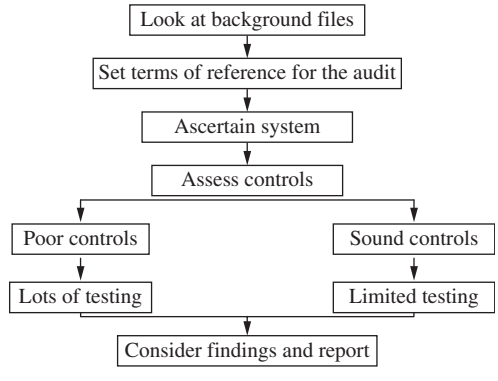


FIGURE 9.6 A block diagram.

One may show the flow of information and the organizational arrangements. The main advantage is that this technique is quick and simple, and sample diagrams can be incorporated within the audit report to aid understanding by outlining the system. For high-level work that does not require a detailed analysis of documentation this can be an efficient way of recording the system. This contrasts with flowcharting where there is an obsession with the detailed movement of documents.

The Rules of Flowcharting

Flowcharts are detailed representations of documents and information that record most parts of a defined operation. The rules that are applied to audit charts are:

1. Provide clear headings and dates so that the system dealt with is clearly identified. Do not make them unnecessarily complicated as this consumes time and may not aid the audit process.

2. Look for exception routines and note these so that a complete picture is provided.
3. Test the flowchart against the client's understanding of the system.
4. Distinguish between operations/processes and controls so that the flowchart can feed directly into the control evaluation procedures.
5. Number the events in sequential order as they may be referred to in other audit working papers.
6. Keep the narrative brief to avoid making the schedule appear cramped.
7. Show destination of all documents by not leaving loose ends.
8. Distinguish between information and documentation flow.
9. Use a convention of moving through the system – top to bottom and from left to right.
10. Apply standardized symbols and keys that are fully agreed and detailed in the audit manual.

Rutteman

The Rutteman convention is popular and tends to be used by ICAEW/ACCA trained auditors:

1. It has fewer symbols than some more detailed flowcharting conventions.
2. It has fewer operations.
3. There is less narrative in the margin.
4. Everything has to be concluded.

Some of the standard symbols used are listed in Figure 9.7.

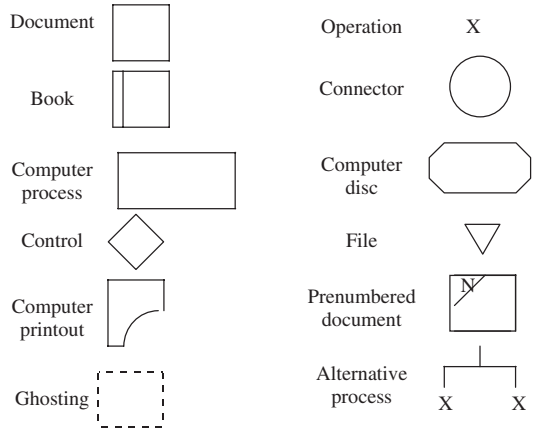


FIGURE 9.7 Standard flowchart symbols.

Documents that have been processed will normally be found in temporary or permanent files. Temporary files are those awaiting further instructions or information to complete the transaction as in Table 9.2.

As a final outcome of all transactions we should find that they:

1. are permanently filed;
2. have left the system;
3. are destroyed.

TABLE 9.2 Files.

	Permanent	*Temporary*
Alphabetic	A	TA
Numerical	N	TN
Date order	D	TD

Ghosting is applied when multi-part documents are used and the separate parts may be subjected to different sequences of operations so that a restatement of each part may be the simplest way to depict these operations. Sequences of operations representing a subroutine may be shown on a separate chart and ghosting can be used to restate the initial document in the chart. As a brief example of this flowcharting convention refer to this narrative in Figure 9.8:

1. weekly requisitions received by buyer from main office (MO);
2. three-part order prepared by buyer;
3. documents sent to accounts where they check the requisitions with the orders;
4. requisitions are filed in date order;
5. orders are entered into purchase ledger.

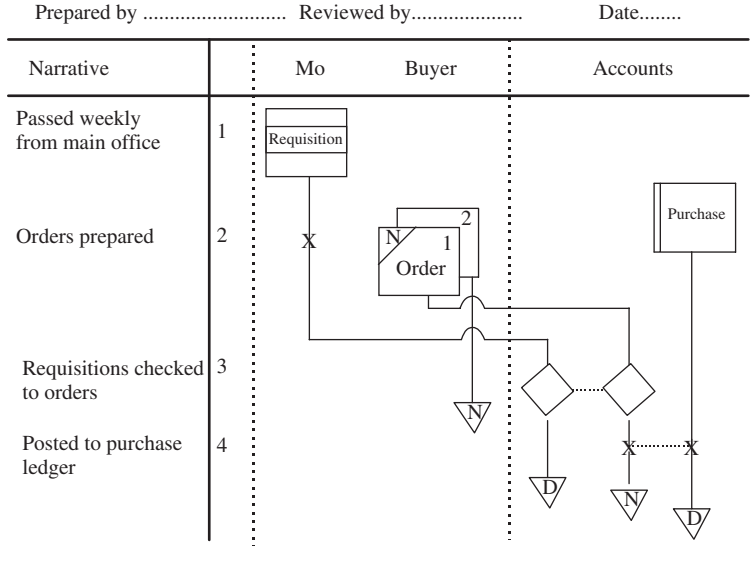


FIGURE 9.8 Ordering system – flowchart.

Pros and Cons of Flowcharting

Main advantages:

- Highlights weak controls particularly relating to a lack of segregation of duties and authorization.
- Indicates possible duplication of work where tasks are repeated.

- Permanent record of the system.
- Shows instances of formal authorization.
- A logical and systematic procedure that can be learnt and applied by all auditors.
- Ensures the complete system is ascertained. Narrative notes may not follow all documents from initiation to conclusion and only by formally charting their flow may gaps be spotted.
- Used to highlight instances of internal check.
- Allows a bird's-eye view of the system.

Disadvantages:

- Training in the techniques required for competent use.
- Time consuming as detailed operations are documented.
- Can be badly drawn and hardly understood by anyone.
- Tends not to be descriptive and suits complicated systems with lots of document flows.
- May be subject to constant change and require updating as systems change.
- Can show excessive detail and become very complicated.
- Becomes an end in itself instead of a tool to be sensibly applied as part of the overall audit process.
- Inappropriate for corporate and managerial systems with high-level controls to be explained rather than charted.

Using the Flowchart

Flowcharts may be used in the following ways:

1. Weak areas or waste of resources may be isolated so that audit attention may be directed towards these parts of the system, or problems can simply be referred to in the report.
2. One can draw a second flowchart to show proposed improvements. The relevant stages may be highlighted in 'before' and 'after' charts that form the basis of discussions with management.
3. One may use the ICQ in conjunction with flowcharts, expanding on areas where there may be systems weaknesses. ICQs are also a form of systems ascertainment in that they relay the control features of the area under review.
4. Walk-through tests may be used to take a small sample of transactions through the system so that the integrity of the documentation may be determined.
5. Automated flowcharting packages may be used.

Balancing the Level of Details Required

There must be balance in the use of ascertainment techniques so that efficiency is maintained and there is perspective involved in applying flowcharting. For the best ascertainment options consider:

- **Narrative** – A simple descriptive overview gleaned directly from the interviews. It should be used wherever possible unless the level of documentation becomes too detailed to deal with in note form.

- **Block diagrams** – Illustrate the main stages of a system and the relationships between components. With the growing use of graphical presentation software, there is scope for attractive diagrams that can be imported into the audit report for ease of reading. Main systems stages have to be summarized for block diagrams to be of any use although the advantage is simplicity in design and ease of use.
- **Detailed flowchart** – These should be used sparingly and only where absolutely necessary. Because of time constraints and the move away from basic operational detail, they have limited use. Where a sensitive system, such as pre-signed cheque ordering, use and dispatch, must be carefully accounted for, monitored and controlled at all stages, detailed flowcharts will probably be required.

Standards on the above including appropriate conventions should be comprehensively dealt with in the audit manual. It is pointless to seek to flowchart in detail all organizational systems as this would be a momentous task. They would need constant change with little or no benefit to the audit service. The choice of ascertainment technique depends on the type of audit and approach adopted. There is a wide variety of available methodologies and this adds to, rather than dilutes, the auditor's skills base. The audit manual is the right vehicle for setting such standards.

9.4 Evaluation

Evaluation may be seen as the most important stage in any audit review since this provides an opportunity for auditors to apply professional creativity to the fullest. The audit opinion and recommendations should flow from the systems weaknesses identified during the systems evaluation. Audit testing routines are carried out to confirm the original evaluation in terms of the application of controls and the effects of control weaknesses.

If the evaluation is flawed then all the remaining audit work will suffer. Audit recommendations will provide substandard solutions to risk exposures.

Defining the system

The preliminary survey establishes which system is being audited. The statement on scope of audit work in the assignment plan will document what is being reviewed and it is this system that will be subject to evaluation. We then have to turn to the model of the system that is being evaluated. The system may be conceived as one of several models:

The prescribed system This perceived version of the system is laid down in procedure notes and official documents. The original systems intentions may be set out in old committee papers and formal reviews commissioned by management. The official description of the system will follow this formally agreed format. The auditor has to be concerned with this system since it may be the one that is officially approved by the organization and if it has altered, then fresh approval may have to be sought. For example, where the organization has agreed to a central purchasing function then any variation to this model, where managers place their own orders, should be formally authorized. If not, we may be in breach of procedure.

The alleged system This follows the procedures that are described by the management and staff operating the system. It allows for any changes to the official system that have been made by operatives over the years. Although the steps that constitute the operational system have been

conveyed by line managers, they may in practice be carried out differently. When the auditor first starts the audit, management will tend to give the 'Rolls-Royce' version of the system in that all work is well managed, supervised and controlled. For example, the manager of payroll may arrange work into three teams and argue that it is well managed and controlled. After a few days' work the auditor may find that each team works to their own standards and as a result the overall payroll operations are fraught with inconsistency and error.

The planned system The system that management wishes to install may be called the planned system. The auditor may be asked not to review the existing operations but concentrate on management's proposal since it is this that will form the future system. On one level it is good to feed into development plans as a way of directing attention at major managerial concerns. The problem with this approach is the uncertainty of futuristic proposals that may simply exist as management ideas. Actual problems that relate to the existing arrangements cannot simply be ignored. For example, a sundry debtors' function that had a poor collection record should be subject to an internal audit. There is no point in managers seeking to abort the planned audit on the basis that they are seeking to resolve the problems. The auditor notes the planned changes but will examine the scope of the problems and whether adequate controls have been or are being installed.

The emergency/contingency system Although the system may be clearly set out and applied on most occasions, there is also an emergency system that the auditor may wish to consider. This is based on the need to 'get things done' in an emergency and may result in many overrides of official procedure. An example is where the organization is making redundancies. Any audit review of controls where the operation is fully staffed and working normally may be irrelevant where everything is subject to major change. Short-cuts may be taken for expediency and these arrangements cannot be ignored. Emergency routes should form part of the system as exception routines and be included within the scope of the audit review. Exceptions create major vulnerabilities in systems as otherwise sound controls may be by-passed, normally by senior management.

The ideal system Published research on systems control and VFM studies, by their nature, use generalizations on how defined operations may be improved. The temptation to set out ideals on systems control may be seen as part of the drive to establishing an 'ideal system'. This can also occur where the package of controls is fine in theory but becomes too cumbersome and complicated in practice. The auditor's recommendations will appear to be out of touch with operational reality if based on ideals that do not attach to actual working practices. This problem arises where the auditor insists on making snap judgements about devising new controls.

The auditor's preferred system The auditor's understanding of the systems processes and control weaknesses may convince him/her that certain improvements are required. These may be seen as the auditor's version of the ideal system. It is not the auditor who will be charged with operating these recommended controls so it must be supported by findings which identify the need for further improvements. Findings are generally obtained through the application of compliance and substantive tests. Marketing and negotiation may be required to 'sell' the audit recommendations.

Staff's preferred system Supervisory staff and front-line employees may have a vision of the type of controls that should be incorporated. The system preferred by management tends to be

what the auditor finds during the review, unless management is not aware of non-compliance or the full implications of control weaknesses. Staff will tend to implant additional checks and records to assist them in their day-to-day work, many of which act as compensating controls. The issue of non-compliance may be related more to conscientious employees devising new routines rather than purposely by-passing formal controls. The auditor must try with caution to capture the real system.

The workable system This is the system that works in practice and retains all the required control features. It may fall somewhere between the ideal system, management's system, audit's preferences and the procedures applied by staff themselves.

The best system The question arises as to what is the best system. There would seem to be several interpretations. The 'best' system is able to contain risks to management's objectives, which brings into play exactly how this criterion should be applied. The starting place is to isolate the success criteria that managers use to guide them in managing resources. We would expect these to coincide with the organization's view of success. Where the internal auditor finds that management has failed to establish performance indicators this is a control weakness. If these indicators would have been reported to a corporate management team forum, they may show what management believes they would show, i.e. a poor result that is indefensible. Audit insistence that performance should be measured may fall upon deaf ears since the organization's needs do not coincide with management's own interests. All systems have interested parties who depend on the services to different extents for different reasons. All systems have in-built constraints that limit the level of service delivered. We must still discover the systems objectives and ensure that the underlying controls promote the achievement of these. Once these have been isolated, the systems may be reviewed. To answer our original question we might argue that by taking a pro-organization stance, the best system will be that which delivers management's objectives and promotes the welfare of the organization. Evaluation will be based on the system that is actually in operation, although reference will be had to development plans and official procedures. Successful evaluation requires that the right techniques are applied in the right way, based on a good understanding of the system. The auditor's understanding of the system should include:

1. **Understanding the needs of the parties who rely on the system.** This not only includes front-line staff and middle managers but all those involved in systems that interface. These may sometimes conflict where one user (say line managers) requires readily available financial information while another (say the accountant) demands a high accuracy rather than speed.
2. **Understanding the adopted success criteria** and what the system is about in terms of the competing factors of quality, timeliness, quantity and value of the system's product against the need to ensure risks to these attributes are managed.
3. **Understanding systems constraints** and the relationship between the cost of risks and benefits of control in containing these risks.

Evaluation Techniques

The system being reviewed is the system being applied in practice in line with management's operational objectives. The evaluation applied should be based on those controls required to ensure systems objectives are achieved with no great loss or inefficiency. Evaluation techniques include:

1. **Flowcharts.** These help identify systems blockages, duplication of effort and segregation of duties along with controls that depend on documentation flows and the way work is organized.

2. **Transactions testing.** By testing transactions one might pick up systems malfunctions that cause error conditions identified by the tests. Where we are able to manipulate large amounts of data, the ability to carry out a limited range of tests quickly arises. This cannot be seen as a systematic evaluation since it does not rely on a full understanding of the operation under review, but leaves matters to chance as samples are selected and examined.
3. **Directed representations.** One cannot deny the usefulness of information provided by persons who have knowledge of the system. If management states that there are defined systems weaknesses at the outset of an audit, one would be ill-advised to ignore this source of information. Complaints from users, operatives, middle management and third parties can provide a short-cut to the evaluation process. One would look for bias in these comments as they could not be taken without some degree of substantiating evidence.
4. **Internal control questionnaires (ICQs).** Dealt with below.
5. **Internal control evaluation system (ICES).** Dealt with below.

Recommendations should be based on dealing with problems as illustrated in Figure 9.9.

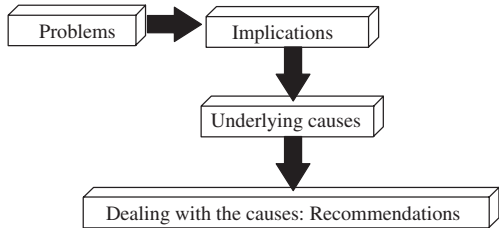


FIGURE 9.9 Evaluation.

At some stage we apply this framework against what we find in practice. This is why the evaluation stage is where the auditor's creative abilities come to the fore.

Internal Control Questionnaires (ICQs)

ICQs are widely used to assist the control evaluation process and there are many standard packages. They consist of a series of questions applied to a particular operation and designed so that a 'no' answer indicates a potential control weakness. One might ask:

> Is the task of receipting income separated from the recording of this income?

The idea being that a 'no' answer may mean that official duties are insufficiently segregated. The potential weaknesses are then further explored and compensatory controls looked for before testing routines are applied. ICQs have a number of specific advantages and disadvantages:

Advantages

1. Provides a permanent record of the evaluation stage. As the schedules are completed they automatically record the response to each key point examined as a ready-made working paper.
2. A disciplined, systematic approach to evaluation not depending on the whims and fancies of the assigned auditor.

3. Helps audit supervisors as the standard of evaluation is set beforehand through compilation of the ICQ. The expectation that field auditors will ensure full coverage of the defined areas via this process provides a useful management tool for controlling the audit.
4. Provides direction to the auditor by setting out clearly the areas that are to be addressed. In this way the auditor can approach an audit armed with the necessary tools, i.e. the ICQ checklists. There is no need to rethink the control mechanisms that form part of the evaluation process as they are set out in the ICQ. The 'what should be' model is then available to be used to assess the adequacy of existing practices. Some might argue that the ICQ provides indispensable guidance.
5. It is simple to use as the questions are directed at control objectives that should be present in the operation under review.
6. The technique can be used by inexperienced auditors who should find it simple to adapt their work to provide responses to the listed questions.
7. It depersonalizes the audit by setting tried, trusted and objective criteria for the controls in operation. The auditor can defend a charge of being too obsessed with control by referring to the ICQ standards adopted by the internal audit function and not devised in a hit-or-miss fashion.
8. ICQs promote a systems-based approach. They emphasize controls as the main source of audit attention, rather than the testing programmes that may be the main basis for the audit. Controls are deemed by the ICQ to accomplish objectives that support the main thrust of the systems approach.
9. Provides good structure and form to the audit by defining beforehand the way systems will be assessed. Planning is easier as time can be assigned to completing the requirements of the ICQ and the work has a natural start and finish in line with the control standards used.
10. It results in comprehensive cover of an area by dealing with all foreseeable points. It is impossible for an auditor to be aware of all control features within an ICQ, particularly the more comprehensive ones. Having the checklist in hand enables one to take on board many factors.

Disadvantages

1. They can lead to a stereotyped approach where each year the auditor seeks to examine a series of predetermined factors that are wholly predictable. It may engender a bureaucratic approach where detailed enquiries are repeated time and time again with little or no real inspiration from the auditor.
2. It can become mechanical as the task of completing the never-ending checklist becomes so laborious that the auditor develops a secret desire to leave the profession.
3. They may be followed blindly by an auditor whose preoccupation is to complete schedules without really understanding why. It is one thing to provide comprehensive direction on audit coverage, but simply to employ form fillers is unacceptable. Where strict time limitations are placed on completing the schedules, there may be little time to think through the actual implications.
4. Detailed ICQs may stifle initiative. The inexperienced auditor may find the detailed guidance useful whereas the more skilled may feel frustration with this mechanical process. The wish to divert resources to new issues that may have been discussed with client management may be impaired by the fixation with the ICQ as documentation that needs to be completed. The professional auditor needs freedom to follow high-level issues to their conclusion as a way of targeting key risks.
5. Management may feel that it is a cumbersome, time-consuming technique. Where the auditor is completing a checklist, which ranges from important matters to immaterial detail on insignificant parts of the system, it may appear amateurish. There will be some parts of the ICQ to be based

on questions to line management and it may be tedious to seek the required responses. Some of the questions may elicit inappropriate answers and some may display poor understanding by the auditor of the systems. Most of these disadvantages arise from a misuse of the ICQ procedure which, at its worst, ends up with the auditor sending a list of 101 questions to management.

There are a several ways that the ICQ technique may be applied more efficiently and effectively:

- Tailor the standardized ICQ to the specific circumstances based on understanding of the system under review. Make each question relevant. Using automated schedules makes this task much easier where the auditor can amend the document on computer disk.
- Gear the questions into control objectives as a way of interfacing them with the system. Once the key control objective has been agreed upon then the questions can be directed to the control issues.

Parts of the ICQ that relate to a stores system appears in Table 9.3.

TABLE 9.3 Control-related ICQ.

Question	*Yes*	*No*	*Test no.*
ORDERING SYSTEM			
CONTROL OBJECTIVE: To ensure that stores are authorized, delivered, correct, safeguarded and available.			
Q.1 Is the person certifying the order independent of the storekeeper?			
Q.2 Are orders placed only with approved suppliers?			
Q.3 Does the order make reference to a purchasing contract?			
Q.4 Are stock level reports issued regularly for reordering purposes?			

Do not give them to the manager to complete but use them for fact-finding discussion. The ICQ should be completed by using all available sources of information from interviews, observation, initial testing, documents, manuals, representations and past audit files. It is compiled as the audit progresses taking on board a wide range of information.

Internal Control Evaluation System (ICES)

The ICES is partly a conceptual model linked directly to the systems-based approach and partly a mechanism for setting out the evaluation process in matrix format. Unlike ICQs it involves setting out the components of good evaluation in a schedule (or matrix) format so that a systematic series of steps can be undertaken before testing, conclusions and recommendation are made. The main headings may appear at the top of the schedule as:

- systems objectives
- control objectives
- risks to the achievement of control objectives
- available control mechanisms

- existing control mechanisms
- initial evaluation
- testing strategy required
- test results
- conclusions
- recommendations.

The entire audit process is established in a formal systematic fashion, although this technique tends to be used by more experienced auditors with a full understanding of the system. Note that this format appears very similar to the risk registers that are prepared through the CRSA process. An example of this audit evaluation approach applied to an audit of a local authority small business grant approval system is given in Table 9.4.

There are several advantages to this approach:

1. It treats controls as part of the process of mitigating risks to achieving objectives; therefore it starts with what management is trying to achieve (i.e. the systems objectives). The entire audit process is seen to flow from this start point.
2. The auditor does not possess a pat answer to controls as suggested by the ICQ approach. It is a question of working out which control objectives are relevant (having regard to the systems objectives) and then seeking to determine which control mechanisms should be in place. This technique is more difficult to master as it requires a commitment to systems auditing. Instead of being armed with a list of questions, the auditor is armed with a database of control mechanisms that fit various risk scenarios.
3. The ICES requires the auditor to analyse the system and break it down into logical components as it flows from input, process through to the final output in chronological order.
4. The ICES deals with control risk and exposures as an extension of the evaluation procedure. This requires a considered understanding of the activities under review. A good appreciation of risk enables the auditor to direct control mechanisms at the right parts of the system.
5. The ICES flows naturally into the testing routines as after compliance has been reviewed, the poorer parts of the system are then subject to substantive testing.
6. The ICES forms a record of control weakness to be placed in front of management and discussed before the draft audit report is prepared. We are able to provide a full audit process encapsulated within the ICES schedules. This contains details of objectives, how existing controls compare with desirable ones, the test results obtained, final opinion and recommended improvements derived from resolving weak controls that were confirmed by tests applied.
7. The ICES means a move away from the old audit programme approach where a list of basic tasks is given to the auditor to work through. This method leads to creative, thinking auditors who can operate more at strategic levels.
8. An even better format may be the integrated audit approach (see Chapter 8) where the business advice would embark on a risk workshop to get to the key risks that would then be used to drive the resulting audit. They would then resume to work through ways forward (rather than audit recommendations) before the audit report and agreed management action plan was prepared and issued in draft.

Evaluation as a Continuous Process

This section has commented on some of the techniques that auditors use when evaluating systems. Although formal evaluation is a clear component of the audit process, it is also a function

TABLE 9.4 Business advice service control evaluation.

System aim – 1. To encourage business regeneration through local grants

Process stage and control objective	*Inherent risks*	*Desirable controls*	*Existing controls*	*Initial assessment*	*Testing strategy ref. and results*	*Audit recommendations*
GRANTS AVAILABLE 1.A Awareness of grant	Little appreciation of grant availability	Wide publicity	Word of mouth only	Inadequate	1.A.1 survey of local businesses Result – awareness poor	1. Need to launch scheme properly
ELIGIBILITY ESTABLISHED 1.B Objective eligibility criteria	Many ineligible businesses applying	Information package	New comprehensive leaflet and website in use	Very comprehensive material	1.B.1 check that applying businesses receive info Result – OK	N/A audit assurances provided
BUSINESSES APPROVED 1.C Meet criteria	Wrong businesses approved	Formal assessment	Subjective selection	Open to abuse	1.C.1 check whether wrong approvals made Result – poor	2. Prepare formal assessment criteria
GRANTS PAID 1.D Pay the correct person	Cheques going astray	ID and collection	Posted out	Can go astray	1.D.1 check that ID system adhered to 1.D.2 cheques received by businesses Result – no fraud	N/A audit assurances provided
BUSINESSES GROW 1.E Effects of grants known	Grants have no impact on local community	Database follow-up	Not done	VFM not assured	1.E.1 examine failure rates of aided businesses Result – poor	3. Monitoring and new tracking system required

that can occur continuously throughout the audit. The final audit opinion will be derived from many factors and information that the auditor uncovers during the audit:

- As flowcharts and systems notes are formulated they indicate systems weaknesses in problem areas. These should be separately noted for future reference when developing a testing programme. It is possible to get an initial impression when, say, touring the location and this adds to the auditor's understanding. If an auditor finds files and documents scattered, these initial impressions may be tested by checking the whereabouts of a selected sample.
- Matters connected with the economy, efficiency and effectiveness of the operation may arise at any time during the audit. They may suggest that management has not taken reasonable steps to ensure they are providing VFM. These are all findings relating to the overall state of controls that may appear in the audit report.
- Systems control objectives will have to be carefully defined in line with management views since this will have a fundamental bearing on the controls that are assessed. Where management has failed to set clear objectives there is little hope that they will have any success in discharging their responsibilities. If there are objectives but they fall out of line with organizational policies then this is a finding in its own right. We can go on to suggest that 'auditing through business objectives' brings the auditor closer to the high-level issues than any other audit procedure. The success criteria and risk management strategy that management apply will guide the auditor in deciding whether the controls are working.
- The objectives of the system and management perception on what is being achieved have to be fully appreciated before controls can be reviewed. This requires the auditor to have a good understanding of the system under review and means management has to be fully involved in the auditor's work.
- An understanding of the available control mechanisms again will assist the evaluation process. Imagine an auditor who has been given a computer notebook that contains the full text of the audit manual. In addition a comprehensive library of control mechanisms would also sit on the hard disk. Having been given terms of reference for the audit and budgeted hours for the job, we would expect that the library of control mechanisms (used in conjunction with the audit manual) would guide the auditor in the most important task of control evaluation.
- The level of existing controls should be assessed as a package that together forms a system of internal control which in turn has to be checked for compliance. The act of obtaining information on the proper functioning of these controls must occur throughout the audit and not just during control evaluation. We would hope that formal control evaluation would provide an opportunity to bring the findings together so that an actual opinion on controls may be provided. One way of summarizing these findings is to relate operational risk to the four key control objectives of reliability and integrity of financial and operational information; effectiveness and efficiency of operations; safeguarding of assets; and compliance with laws, regulations, and contracts.
- Fraud is usually an indicator of poor control and where this has occurred in the past, the evaluation should be carried out with a view to preventing similar control breaches that might facilitate fraudulent activity. As such, matters relating to past frauds should be brought into play when considering the adequacy of the entire system of internal controls.
- Compensating controls may be used by operatives where formal controls are inadequate in containing risk or are not used in practice. They may be organic in nature and if formally adopted, may be more effective than official procedures. Key controls are fundamental control mechanisms that have to be in place as opposed to less material optional control features. An example of a key control is regular feedback for managers on operational performance.

- The whole control environment including the operational culture will have an impact on the way control mechanisms are defined and adopted. If the auditor ignores this then the evaluation will be substandard. An ICQ approach is better able to deal with assessing the control environment while the ICES copes better with assessing risk in systems and processes that can be broken down into clear stages.

During control evaluation the auditor's judgement is perhaps the single most important factor and this will be based on experience and training. The whole process of reviewing the system will arise throughout the audit and the formal evaluation techniques may be used to confirm the auditor's initial opinion. Control findings have to be tested. First, they must be checked to see if controls are being applied as intended. Second, the effects of weaknesses must be established and quantified as Figure 9.10 demonstrates.

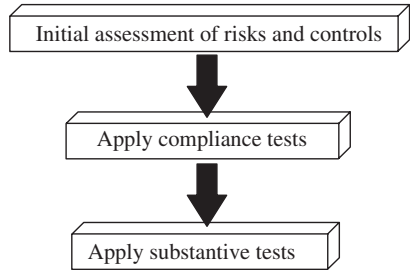


FIGURE 9.10 Evaluation confirmation cycle.

A Perspective on Control Evaluation – by Richard Todd

Richard has prepared the following paper for *The Internal Auditing Handbook*:

Introduction: Control evaluation is a key area within the review process, which has to be undertaken meticulously in order to remain on track and consonant with the audit terms of reference. The audit objectives must be transposed into several subliminal control objectives. This may seem somewhat obvious to most but in practice this is an area that can cause problems. But in practice what are we really looking for from the control evaluation process and why is it so important? The control evaluation process in practice is the determination of control objective in line with the audit brief and assessing the relational expected controls against the actual controls.

Audit brief: Given the nature and diversity of organizational systems nowadays it is commonplace for the audit brief to focus on an element of the system. A classic example of this is a payroll system. A payroll system will have several subsystems;

- Starters
- Leavers
- Sickness payments
- Tax deductions
- Pensions payments
- Gross pay

In larger organizations any one of the above areas will form the basis of a ten-day audit, very rarely will the auditor be asked to review the payroll system as a whole in such an organization. Conversely in smaller organizations it is very conceivable that the audit will be asked to review the payroll system in its entirety.

Terms of reference for a payroll audit 'to review the adequacy and effectiveness of the payroll starters and leavers' a ten-day audit to be completed by 00/00/00.

The next stage is to break down the TOR to manageable control objectives. Many auditors at this point opt for professionally produced Internal Control Questionnaires (ICQ). In the recent years I have seen greater use of ICQs, which is useful, as an aide mémoire, but I feel it should not be used in isolation. The auditor must have a defined evaluation approach, which focuses the mind on the subject matter. But the approach that I like is what I call the system breakdown approach. Outlined below is a blockchart showing the process involved in Figure 9.11.

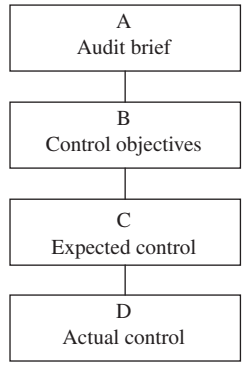


FIGURE 9.11 System evaluation approach.

Under my 'breakdown approach' let us now define the relationship between the various stages of control evaluation.

- Terms of reference to control objectives can be expressed as A = nB, n being number of observations.
- Control objectives to expected controls can be expressed as B = nC, n being the number of observations.
- Control weakness can be expressed as D = nC – nD

Having determined the audit brief the next stage is developing the control objectives in line with the audit brief. This is where I divide the system into input, processing, and output control. Every system by its very nature must consist of these three steps, after all a system is there to achieve some output or some conclusion as in Figure 9.12.

- Input controls are those controls that are activated prior to the processing of the transaction.
- Processing controls are those activities that change the state of the data, record, or operation.
- Output controls are those activities that are activated after processing has taken place.

Getting back to our terms of reference of payroll starters and leavers, what input control would we expect?

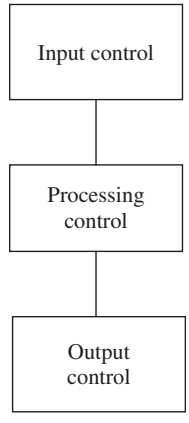


FIGURE 9.12 Systems control.

Input control objective:

- That all new starters are correctly authorized in line with the organization scheme of delegation, and that there is adequate supervision over the process.
- That all new starters have been appropriately vetted.
- That all leavers are correctly authorized in line with the organization scheme of delegation.

Processing controls:

- That all new starters' details are correctly entered on the payroll system in a timely fashion.
- That all new starters are associated with the correct cost centre for financial control purposes.
- That all new starters are formally recorded in the organizational staff register.
- That all leavers' details are correctly and promptly deleted from the live payroll system in a timely fashion.

Output controls:

- That there are control reports produced by the payroll system listing all new starters and leavers processed on the system in the control period under scrutiny.
- That all starter and leaver reports produced by the payroll system are reviewed by someone not involved in the processing.
- The above listed control objectives are not exhaustive, rather they are designed to highlight the audit thought process in breaking down the original terms of reference into subliminal control objectives.

The above stated control objectives now form the platform for the control evaluation process. This is the process of moving the control objectives to expected controls and matching them to actual controls and report of the variances. Most large internal audit departments now have a standard format setting out the evaluation process.

Let's now take a control objective and break it down to expected controls.

Control objective: Let's now take one of the control objectives and cascade down to expected controls.

- That all new starters are correctly authorized in line with the organization scheme of delegation, and that there is adequate supervision over the process.

Expected control:

- That an authorized signature list exists.
- That all starters and leavers are duly authorized by a member of staff with the delegated authority as per the authorized signature list.
- The member of staff authorizing the new starter is not involved in the recruitment process.

Actual controls are those controls the auditor finds during the course of the audit field work either when ascertaining the system or as a result of testing.

Common mistakes:

- Some auditors prefer to follow the proverbial audit nose which means in practice there is no defined methodology; rather the auditor uses his/her empirical experience to focus on vulnerable high risk areas.
- Some auditors don't take time to evaluate the controls properly.
- Some auditors stick religiously to ICQ and tend to be lost without it.
- Other auditors don't always ensure that the control objectives are consonant with the audit brief.
- Some audit sections have too much standard audit documents surrounding the evaluation process. This can lead to a robotic approach to the audit and it serves to suppress the audit flair.
- Other auditors reproduce the work done in previous reviews.

Good practice:

- The terms of reference or audit brief must fully understood by the auditor prior to planning the audit.
- The auditor must have a clearly defined approach to evaluating risk and control, and in so doing should take time to plan the audit effectively. Many organizations will have standard formats for controlling the approach. However, where this is the case the chief internal auditor must ensure that the standard formats are not dictatorial or intrusive as this will only serve to frustrate and dissuade the experienced auditor.
- The auditor must always be mindful of time constraints when drafting the control objectives; to this end the auditor must focus on the key controls considered so fundamental to the system of control. If we hark back to our payroll example what would we consider a key control? Those all new starters are authorized by someone with the delegated authority to do so. If this were not the case how would management be in a position to be assured of the integrity of the payroll? The danger of the infamous ghost on the payroll would loom large.
- Systems notes and testing results must fully support actual controls found.

A well-constructed control evaluation will indeed go some way to writing the report, in fact the wording used should be such that it can be lifted in its entirety and placed in the body of the audit report; this will serve to avoid duplication and reduce audit reporting time. Having said all this about the control evaluation process, the client generally does not care about this: they are only concerned with findings. I have worked in many organizations and I have never been asked about the methodology or approach; what I am challenged on from time to time is my findings. The auditor should never lose sight of that. End-product findings, recommendations and conclusions are what the client is paying for and are what ultimately the success of the auditor will be judged by. In all the organizations I have worked for there has been a different approach to control evaluation; but they all had a common theme. In practice it is mastering the common theme that is key.

9.5 Testing Strategies

Testing is the act of securing suitable evidence to support an audit. It confirms the auditor's initial opinion on the state of internal controls. It is a step in control evaluation, although many auditors test for the sole purpose of highlighting errors or non-adherence with laid down procedure. It depends on the audit objective. The IIA Practice Advisory 2240-1 requires audit procedures to be in place to ensure the required evidence can be gathered:

> Internal auditors develop and obtain documented approval of work programs before commencing the internal audit engagement. The work program includes methodologies to be used, such as technology-based audit and sampling techniques.
>
> The process of collecting, analyzing, interpreting, and documenting information is to be supervised to provide reasonable assurance that engagement objectives are met and that the internal auditor's objectivity is maintained.

The Testing Process

The auditor should gather sufficient evidence to support audit findings. This means the information should be factual, adequate and convincing so that a prudent, informed person would reach the same conclusions as the auditor. Competent information is reliable and the best attainable through the use of appropriate engagement techniques. Relevant information supports engagement observations and recommendations and is consistent with the objectives for the engagement. Useful information helps the organization meet its goals.

The testing process is illustrated in Figure 9.13.

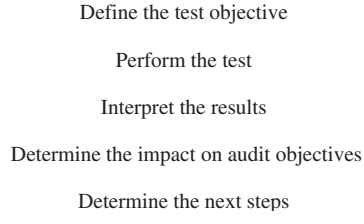


FIGURE 9.13 The testing process.

Brief explanations follow:

Define the test objective There must be a clear reason for performing the test. In systems auditing this relates to the adequacy or effectiveness of controls. For example, if we are concerned that there is no proper system for ensuring that orders are properly authorized, then we may examine a sample of orders to see if they comply with the purchasing code of practice. The test objective is to judge the extent of problems.

Define the testing strategy How test objectives are achieved is determined by the testing strategy. This lists the tests required and groups them to aid their efficient execution. If we need to examine application forms for a sample of newly recruited employees as part of an audit of personnel procedures, we need to decide how this will be best achieved, the use of statistical sampling and how data will be extracted.

Formulate an audit programme The testing strategy can be defined in more detail and form an audit programme of work. This programme becomes a schedule containing space for the samples to be listed and the tests performed and documented. It provides a ready-made guide to the completion of the testing strategies. The programme may appear in matrix format with space on the left for a list of payments made to subcontractors that are selected at random. The rest of the schedule will be broken down into columns for each part of the tests. This could cover checks over order, contract number, payments, certificates, invoices, select list of suppliers, budget provision and tax exemption. This checks whether procedures over the employment and payment of subcontractors work.

Perform the test The detailed work of performing the tests is the main part of the testing process. The key point is that there is a tendency for the test objective to be lost in the vast amount of work that may be required during the test performance stage.

Schedule the evidence The results of testing should be summarized and fed into the report (via the ICES) and be cross-referenced in the working papers. Test results give an overview of results, and provide detailed schedules that may be sent to management for action. They may be referred to in the audit report as examples of actual problems. Where we have examined hundreds of payroll payments and found several categories of errors (say the wrong pay rates applied) we may mention the amount of over/underpayments in each department in the report. The working papers should assist by allowing summaries to be compiled without extra effort. Interesting examples may be highlighted and the design of schedules should enable these items to be readily extracted.

Interpret the results The meaning of what is found feeds into the testing strategy. If we examine a series of performance reports for indications of misleading information being provided, we must have set criteria against which to measure findings. We must consider whether what was found is accurate and have access to a suitable model to make this judgement. If we check authorizations for new accounts on a computer system, the checks will only make sense if we have a list of authorizing officers. Interpretation is based on evidence not rough assumptions and Mike J. Novak has a view on making assumptions:

> At some time or another, probably every member of audit management has wished for one ultimate power – the prerogative to fire any auditor who uses those dreaded words, 'I assumed . . . '. The audit work looks good. Controls appear to be in place, and all bases have been covered; but a closer look suggests that something doesn't quite make sense. You talk to the auditor and ask what the auditee had to say. The auditor answers, 'Well, I didn't ask that particular question, but I assumed it was handled this way.' We all make assumptions, of course. To assume, meaning 'to take for granted as fact', is a basic premise of auditing; but it's imperative that we make those assumptions based on sufficient facts and appropriate analysis. We often think we have the facts and don't; and, as a result, we may arrive at the wrong conclusions.[5]

Determine the impact on audit objectives The link back to the original objectives should be firmly in place so that we take the mass of data and decide what it means for the audit. Auditors should give an opinion on areas covered. This will be based on the state of controls and whether this led to unacceptable levels of risk being identified through testing. This part of the testing puts the detailed work into perspective by providing an outcome. This cannot be to list errors found by internal audit, since this would be for management to do. The goal is to support an audit view of risk management and controls resulting in a recommendation. We would want to see that the

operation in question is properly aligned to corporate values and in both audit and consulting work, this is an important consideration as laid out in IIA Performance Standards **2110:**

> The internal audit activity must assess and make appropriate recommendations for improving the governance process in its accomplishment of the following objectives:
>
> - Promoting appropriate ethics and values within the organization;
> - Ensuring effective organizational performance management and accountability;
> - Communicating risk and control information to appropriate areas of the organization; and
> - Coordinating the activities of and communicating information among the board, external and internal auditors, and management.

Determine the next step Taking into account all that has been found, the direction of the audit should be agreed particularly if there is a need to change plans. One outcome may be to extend the testing routines into greater detail or other areas, or ask management to look into particular problems. We may find matters that were totally unexpected and there must be opportunity to review the audit and current position before going headlong into the next stage of the project.

The Four Types of Tests

Walk-through This involves taking a small sample of items that are traced through the system to ensure that the auditor understands the system. It occurs during the ascertainment stage of the audit and may lead into further tests later. The client may be asked to refer to named documents representative of the transaction cycle that will be cross-referenced to the interview record to assist this process of 'capturing' the system.

Compliance This determines whether key controls are adhered to. It uncovers non-compliance or unclear procedures. If key controls are not being applied, and this is not compensated for by the system, they become reclassified as weak controls. Note that internal auditors should review operations and programmes to ascertain the extent to which results are consistent with established goals and objectives to determine whether operations are being performed as intended.

Substantive These determine whether control objectives are being achieved. Weak controls imply objectives will not be achieved and substantive tests are designed to confirm this initial audit view on the impact of residual risk. Substantive tests may isolate risks that materialize in the form of error, poor information, direct loss or poor VFM.

Dual purpose This is not a test but a recognition of the practicalities of testing controls where one may wish to combine compliance and substantive testing. An example is to examine an invoice that is certified for payment (compliance test) and is valid (substantive test). It would be impractical to select this invoice twice for two different tests to be separately applied.

The important tests are deemed to be compliance or substantive as these are the two main techniques used to support audit work. The relationship between the four tests is shown in Figure 9.14.

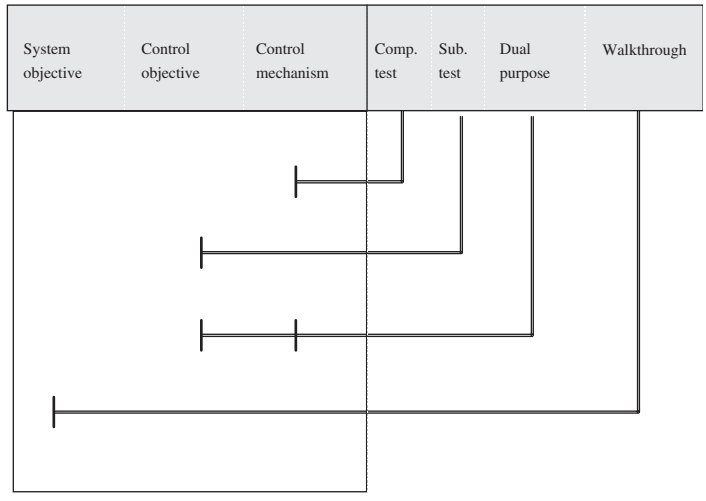


FIGURE 9.14 The various test patterns.

We summarize our discussion:

- Walk-through tests seek to determine how the system's objectives are achieved.
- Compliance tests seek to determine whether control mechanisms are being applied.
- Substantive tests seek to determine whether control objectives are being achieved.
- Dual purpose tests check for both compliance and actual error, abuse or inefficiency.

Comparing Compliance and Substantive Tests

There are key differences between the two main types of tests. We restate the systems-based approach to auditing and how these tests fit into the audit process in Figure 9.15.

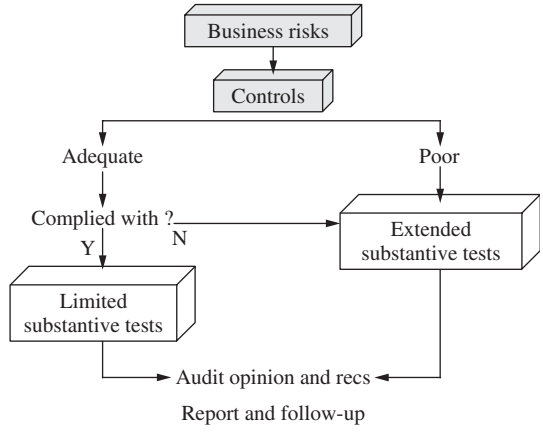


FIGURE 9.15 Compliance and substantive tests.

We look first for compliance with key controls then review results. Substantive tests are then directed towards all known weak areas including those where key controls are not being observed or revealed through compliance testing.

Testing Considerations

The decision on what to test and the extent of testing will be based on factors revolving around evaluation of the systems of internal control. The internal auditor will need to secure sufficient information to complete the audit and ensure that this information is factual, adequate and convincing so that a prudent, informed person would reach the same conclusions as the auditor. Testing considerations include:

The relative risks The type of risks that arise where a system of control is inadequate or compliance is essential is the most important consideration in testing. The parts of the operation that are risky should be targeted for more testing than less sensitive parts. Where a payments system requires an additional signature for items over £1 million this procedure becomes important and must be adhered to because of the large sums involved.

Management needs Where management has concerns about aspects of the system this should feed into the testing strategy. If in a large debtors system, senior management is concerned that staff may be suspending reminders where there is a query on the account without first investigating the matter, this may be explored by internal audit. We would want to see sensible controls installed over the process of stopping routine reminders as a long-term solution, but to establish the extent of this problem, some audit testing may be carried out beforehand.

Previous audit cover The types of findings that were obtained in previous audits can assist planning tests in the latest review. This information may indicate areas of concern and areas where no real problems were found in the past. Testing can be used to support a follow-up of a previous audit. We can establish whether data are being entered onto systems in a disciplined fashion or haphazardly as identified in the previous audit.

The auditor's own experiences The auditor may have come across systems in the past where there were certain parts that presented a difficulty. This may relate to the difficulty in retrieving past years' data where they had been archived.

The level of managerial support for the audit One key factor in setting testing levels is related to the position assumed by management in respect of the audit. Where top management is aware of significant risk and is openly seeking advice from internal audit, there is little point in proving in detail that these problems exist. Test results will set the context of any required action by highlighting how bad the true position is, from the sample examined. Where no one needs convincing that there are real risks to the business, the emphasis will be located with the recommendations and not the evidence from testing. The auditor must convince him/herself by performing some tests but there is little use in doing detailed work when all sides agree on the main control issues. The IIA Performance Standard 2320 confirms the importance of testing: 'Internal auditors should base conclusions and engagement results on appropriate analysis and evaluations'.

The availability of evidence Testing starts from a hypothetical view of control problems and efforts to substantiate initial findings can look good on paper but be difficult to apply in practice. Where evidence is hard to obtain and analyse, this must be catered for when developing testing plans. All tests take time and no audit unit has the luxury of an open budget for 'exploring issues'. Time spent on testing is normally fixed and where information or documents are hard to find, parts of test plans will have to be tailored to this. If the auditor is unable to comment because of such problems then the report will indicate this. Where evidence is withheld we enter the remit of fraud investigations. *Brink's Modern Internal Auditing* makes an interesting point regarding the extent to which the auditor may gather evidence through a spectrum from total ignorance through to complete knowledge as the audit progresses and makes the point that: 'An auditor needs to accept some risk when making a choice of how much evidence to examine'.[6]

The audit objectives Much testing work depends on what one is trying to achieve in line with the stated audit objective. If we need independent third-party verification to discharge the audit objective, say in confirming bank balances, then tests will reflect this. Sawyer makes clear the importance of good evidence: 'Conclusions must be buttressed by the facts. Conclusions are professional judgements, not a reciting of details. Conclusions should present potential courses of action and point out that the cost of correcting the defects will be exceeded by the benefits. The extent of losses shown in the effects is a springboard to the need for corrective action'.[7]

The level of materiality of the item reviewed In addition to dealing with high risk matters we are also concerned that we take on board materiality. When reviewing a purchasing system there is little point checking small-value items that really have no significance to the entire operation as this detracts resources from the more important areas. An audit of a multi-million pound cashiering operation will have little concern for a £50 petty cash float administered by the system.

The time available for the tests The more time available, the more transactions can be tested. There is a bottom-line position that states that time spent on one audit equals time not spent on another. We cannot go on extending tests because there are problems in one area. Testing always takes longer than planned and there must be a cut-off that indicates enough material to go to print.

The assessment of internal control This has to be included as the correct answer to the issue of extent and direction of testing. Testing is required to support an opinion on controls; for example, whether they work, are sound, stop error, stop fraud, promote efficiencies and assist in the proper management of resources. Testing will only be relevant when attached to a clear view of controls.

Analytical Review

Analytical review is a technique that tends to be applied by external auditors and there is an APB statement on this. This involves looking at two or more sets of comparable information, say two years' balance sheets, and extracting new data that can be used to direct audit attention towards areas of particular interest. The use of analytical techniques is illustrated in Appendix D. One would be looking for:

- changes in key ratios;
- absolute changes in key figures;

- general trends;
- movement in the level of purchases and creditors;
- movement in the cash and bank account balances;
- movement in sales and debtors.

The main question that is posed is:

> Are these trends consistent with one another and the overall performance of the organization?'

This directs the auditors' attention towards areas for investigation, although because of the emphasis in comparing financial data the technique is mainly used by external auditors.

Testing Techniques

There are many ways that one can gather the necessary evidence to support the testing objective. The number and types of techniques are limited only by the imagination of the auditor:

Re-performance Rechecking a calculation or procedure can give evidence as to its reliability. This enables the auditor to comment directly on the accuracy by which transactions are processed although it does depend on the auditor being able to perform the necessary task. As an example we might wish to recalculate the amount of money paid to staff who are made compulsorily redundant to ensure that controls, such as supervisory review over payments, are working properly.

Observation This is a useful method of information gathering since it is obtained first-hand by the auditor. There are drawbacks in that what is presented to the auditor may be stage-managed, although this may be a somewhat cynical view. For example, during one audit staff were observed exchanging passwords where they were already keyed into a terminal under their own password and wanted to use another terminal, which was a clear breach of procedure. Structured observation may be used to check controls that have a physical presence such as security and, for example, this may be used to check how cashiers carry out their end-of-day cash balancing operations.

Corroboration Having facts from one area confirmed by reference to another party is a good way of verifying the accuracy of these facts. The more independent the third party the more reliable the results. This technique should be used with care as it should not be an obvious act of rechecking what has been said elsewhere and is best used to follow the natural flow of a system. For example, a payment can be written off by an officer who has placed a stop on the cheque, by writing a memo to a financial controller. Meanwhile, the financial controller should be asked to confirm this, as he/she is visited as part of the audit.

Analytical review Referred to above.

Inspection This is a formal way of observing physical attributes against a set criterion. It implies the use of an amount of expertise to discharge this exercise that the auditor may or may not possess. One might imagine the auditor wishing to inspect building work done by subcontractors that has been certified and paid for by the organization. Again the auditor will not necessarily be

able to carry out this inspection but may commission a consultant to make the required checks and provide a status report. In this case controls over the work certification process can be reviewed through this process of examining previous building jobs. Inspection can also be used to check the existence of assets that have been acquired by the organization.

Reconciliation The process of balancing one set of figures back to another is based mainly on the principle of double-entry bookkeeping that ensures the accounts balance at all times. The reconciliation may be something that is done by management as part of its normal work and this may be reviewed by the auditor using re-performance where necessary. It is also possible for the auditor to perform a new reconciliation to provide evidence of the adequacy of controls. For example, the auditor may seek to balance payroll to personnel systems to establish how well these two systems interface. Any discrepancies may indicate a breakdown of communications between the two functions that could lead to real or potential loss to the organization.

Expert opinion This is less a technique and more a source of assistance linked to another technique. There are many times when the auditor has a problem in terms of securing relevant evidence pertinent to the audit at hand but being unable to perform the underlying work. For example, a stores audit may disclose losses on fuel that management argues is due to the natural process of evaporation. The extent of these losses, having reference to this factor, may be reviewed for consistency by an expert who would examine the facilities and provide an opinion on the validity of the stated argument. The auditor in turn may then be able to comment on the state of controls over safeguarding fuel from unauthorized removal, where there are clear losses that cannot be fully explained through evaporation.

Interviews More often than not the best way to find something out is simply to ask and much useful information can be obtained through the interview forum. This facility is extremely convenient, although the reliability of representations can vary, depending on the circumstances. Where persons provide information this must be verified as far as possible by asking for the document, report, policy, memorandum, minutes and so on that should support what is being said. There are some pointers that are simple to examine, where, for example, we wish to discover whether managers are using the organization's financial regulations. If they are asked whether they possess a copy and cannot find one, then we can argue that they do not make reference to this document in their everyday work. If some of them have never heard of the regulation then we may comment adversely on the adequacy with which this procedure has been implemented in the organization.

Review of published reports/research Another source of supportive evidence is to be found in reports that impact on the area under review. These can range from internal reports, say on staffing levels, externally commissioned reviews of, for example, the potential for new IT, or national reports that contain relevant base data on, say, productivity levels. They may provide information that may be referred to in the audit report covering, for instance, the average cost per employee of payroll services. Alternatively, the existence of a report may simply be used as evidence that management had access to specific advice, that may or may not have been acted on. Any matter raised by the external auditors may also be of use when seeking material to support the internal audit opinion. Obviously reports must be used with care, since the auditor cannot verify the contents of most reports unless prepared from official sources (e.g. government statistics).

Independent confirmation An obvious source of evidence is to get someone to independently agree to defined facts. Where opinion is involved this becomes more difficult as subjective matters can be interpreted in different ways. Direct facts relating to dates, times, figures, agreements and so on can be readily double-checked. The usual example of this technique is debtors' circularization where moneys due to the organization are confirmed by writing direct to the debtor in question. This is a useful device for the external auditor during asset verification. Independent verification may involve checking a representation made by the independent third party. So a stocktaker's certificate may be checked for authenticity by contacting the firm that has issued the document. The rule that the best evidence comes from people who have no vested interest in providing incorrect information is applied. However, this is not a way of viewing all others as somehow untrustworthy, but simply part of the drive to seek the best evidence wherever possible.

Receiving the service as a client Most operations that produce goods or services recognize the key concept of client care that means there must be a net value from what is being delivered. If we were going to audit McDonald's restaurants, the first thing to do would be to purchase a meal from the outlet. Taking this further it is possible to visit or phone and experience the service as a client to obtain a feel for the way controls over this service are operating. If, for example, a line manager has said that all clients receive a complaints form so that feedback is obtained where the service user has experienced a problem, we can find out if this is the case. This technique may be used in conjunction with observation so that an overall impression can be gleaned. We would not be able to refer directly to evidence from this source but it may be used to concentrate attention in the direction of service delivery, if this suggests a breakdown in controls. The approach is not always possible to use but where it can be, it gives an important 'feel' for the operation.

Mathematical models The auditor may construct a model that may be used to gauge particular features of an operation. This is generally not easy as there is a set-up cost involved and the question of credibility when it is used to support an audit report. However, where we have a large audit where it is possible to apply conceptual models, this is a consideration. The example that students will see in most textbooks relates to setting reorder levels in a stores environment. Here the auditor may use a suitable model to test whether controls over stock reordering result in acceptable reorder quantities and frequencies. Other factors such as slow-moving stock and stock-outs will also come into play to support or not support the findings from such a mathematical model.

Questionnaires Formal surveys can be used to assist the audit process. This is a useful device in the audit of an operation that has equivalents either within the organization or in other comparable ones. Because an organization does things differently from other bodies does not mean that this is wrong or right. Telephone surveys can be used to save time so long as full records are made and important matters separately verified in writing. We can elicit data on staffing levels, decentralized operations, use of new IT and other matters from asking questions from other services. We can compute averages and trends to be used to assess the existing position. These devices are best used for more comprehensive reviews that examine controls over VFM.

Comparison Vouching comes under this heading in that we can seek to check one item against another which has an associated factor. There is little that can be said about comparison over and above the basic checking of two or more facts (usually documents). One point to note is that the auditor should maintain accurate records of these comparisons as they may be challenged at

a later date. Furthermore where there is a discrepancy we would have to discover which item is wrong before such matters can be reported. We should also bring the actual error to the attention of management if it is material in terms of the need to make corrections.

User satisfaction surveys Obtaining direct feedback from persons who use the service/product delivered by the operation under review can provide an insight into the success or otherwise of the operation. These mainly test controls over the marketing function attached to the operation. In addition, they can provide a commentary on the QA procedures that have been installed (these QA procedures would be deemed a key control). Such surveys can reveal much more than hours of conversations with management, as they should give a completely unbiased view of the service being audited.

We have already suggested that there is an open-ended list of testing techniques, although whatever techniques are applied it is important to record all results carefully. Clearly, testing is not just limited to basic financial systems but can be applied in any environment. For some of the more sensitive ones, such as the client satisfaction survey, the auditor should make it clear to management that the exercise is being undertaken. Copies of the pro forma documentation that is being used for the purpose should also be provided. Whatever the approach we must be cautious not to appear as spies, performing some type of undercover work, as this will probably impair the audit image.

Achieving Control Objectives

Tests check that control objectives are being achieved. This helps confirm the auditor's view of those controls that need improving and helps quantify the extent of the problem. Control objectives ensure that the systems objectives are achieved with regard to:

- the information systems;
- the extent of compliance;
- safeguarding assets;
- value for money.

When applying test results to determine if control objectives are achieved the auditor should consider:

The success criteria management is applying There is often a conflict between factors the auditor would look for when judging the success of a system. These range from timeliness, accuracy, presentation, client feedback, to performance targets. Not all these will be achieved at the same time. More important is the view of management success. Tests that highlight whether business objectives are being met must include the different interpretations of objectives. There is little point reporting that 2% of time sheets are not reviewed when management feels it so immaterial as not to be worthy of attention. The auditor should ask the important question, whether the control objectives promote management systems objectives. An example may help:

> An auditor reviewed the database for a pension administration scheme and found the details on employees' personal circumstances out of date. This was pursued with management who did not appear overly concerned. The auditor was not aware that the system was designed to

hold historical data to be updated when an employee retired or left. Management's success criterion was based on getting the correct data quickly once it was clear that an employee was due to leave. It was not based on having a well-maintained database at all times.

Any systems constraints There are always constraints over how a system operates. This may relate to resource levels, the availability of information, unforeseeable circumstances and computer downtime. These lead to lack of clarity in the basic formula that reads 'resources given direction allow one to achieve objectives'. The formula becomes more akin to 'resources given direction, notwithstanding problems, allow one to seek to achieve objectives'. Test results that do not cater for the realities of business life will not be taken seriously by management.

The extent of achievement The auditor should recognize that there is no such thing as 100% perfection in any business system. All systems have some imperfection that results in 'error conditions' discovered through audit testing. These errors may not have a significant effect on the performance of the operation and can be tolerated by management. An obsession with these minor infringements can lead to a frustrating audit report that is immersed in the 'findings' without any understanding of the real issues that confront management. Reports that put this into perspective will be better received. There are many managers who receive audit reports that emphasize the results of audit testing by asking what the implications of the audit reports are. The 'points sheet' approach adopted by some auditors can be misguided as the frantic search for errors makes it difficult to distinguish between important and irrelevant mistakes. Findings that have been exaggerated or appear to be insignificant may nonetheless be discussed in terms of the sample that was considered. The key question is to ask whether the sample used is representative of the whole position.

The need to secure good evidence for an audit opinion Testing provides direct material that can underwrite the audit report and conclusions that are contained therein. This is the proper relationship where detailed research backs up the action the auditor believes should be taken in seeking to develop better control systems. The imbalance lies where evidence from testing is secured and presented for its own sake, in the guise of a detailed report on audit findings. One technique that promotes a wider view of the role of testing is to stand back from the specific test results and ask how the various problems relate to underlying causes. This can be used to identify the cause, effect and solution relationship. This enables one to adopt a broader view of the system and how it can be improved. Instead of designing an audit report to read findings and recommendations, we would take findings, draw general conclusions, then provide suitable recommendations based on the wider picture has shown in Figure 9.16.

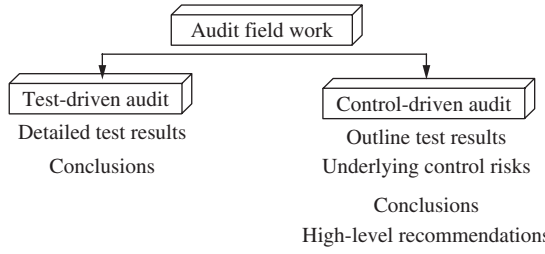


FIGURE 9.16 Putting testing into perspective.

The idea is to gather the test findings into control issues in a compartmentalized manner, so that we may form a view not on the testing itself, but more on the underlying control implications. A lack of clear operational standards may lead to inconsistent work that promotes errors and oversights by staff. Rather than discuss how each error may be corrected, we may deal with the root problem.

The 100% Interrogation Theory

We need to deal with an important development that has growing support and is changing the direction of internal audit. This is the '100% test result' where the auditor uses automated techniques to examine all relevant data on a database. Designated fields are downloaded onto disk and the data manipulated using a package such as IDEA. The audit role becomes testing, testing and more testing in a search for errors, inconsistencies, non-compliance, duplicates, unauthorized items, missing data, incorrect input and suspect transactions. The view is that the audit occurs during this testing. This replaces the systems approach where controls are ascertained and evaluated with testing being seen as a minor stage. The fact that large databases are readily accessible makes this a real proposal with most of the audit work being done at a networked PC as data are interrogated. The flaws in the '100% test result' approach can be noted in a series of relevant questions:

What about the control implications? Testing may isolate specific errors and problems that are being targeted. The findings enable us to comment on the errors that are found but it is more difficult to relate these errors to a failing in the way risk is controlled. An example follows:

> An audit of a contributory pension scheme found that data on employees were being exchanged through comments shouted across the office between the payroll and pension contributions section, located next to each other. A key control of a formal document representing information flows between the two sections was missing. This control weakness was identified through control evaluation. Tests applied to the audit included an attempt to reconcile the two databases (payroll and pensions administration) to identify any discrepancies. These tests could be directed at fields affected by the control weakness, i.e. those that contain data that are exchanged, and we might then comment on the lack of formal section interface regardless of the test results. If the reconciliations were applied blindfolded, without the control evaluation stage, we would end up with a list of errors but no indication of how this happened. We may even find that there are no errors, which does not mean that we cannot report the weakness.

What about managerial arrangements? A large proportion of control is located in the managerial processes that should be in place before we can be said to be in control. These controls are set within the task of setting objectives and directing resources to meet these goals. One strategic goal may be to provide an automated interface between payroll and pension contributions. A list of discrepancies between the two systems is only of use if put within the context of managerial strategies for addressing the issue. The key difference between managerial deficiencies that result in problems, and problems discovered out of context, is that the former enables one to comment on real managerial issues. The interpretation of test results that are derived from extensive interrogation techniques is very difficult if these tests have not been directed at control issues. The relationship between managerial arrangements and detailed

reports from database interrogations can only be established from a top downwards approach. The information system and data that are contained there are only one minor part of the operation and only support the services that are being delivered. Auditors immersed in the analysis of these data will have little time for the real performance issues. The 100% interrogation approach stems from the external audit view that seeks to verify the accuracy and fairness of financial information. An obsession with this approach stops the internal auditor from rising above the external audit perspective to assume the expanded role of an independent risk management systems and control consultant.

What is management's role? Audit interrogations of the vast bulk of computerized data are designed to isolate matters of audit interest. If this interest is to support findings concerning how management has organized systems of control, then we can argue that this is the audit role. If this interest is in discovering errors or inconsistencies in the data that are processed we will have to suggest that this is part of management's responsibilities. Any attempt to remove the role of ensuring the integrity of the database from them will dilute managers' power and motivation. Any attempt to show managers how poor their data are, again is something that should be performed by managers themselves. At the extreme we can suggest that the auditor is being selfish by not passing over interrogation software to management and allowing it to carry out 'cleansing' procedures.

What about following up problems? One problem when the auditor prints out a series of 'suspect items' is that of follow-up. We come across the enigma of working out how to uncover the meaning of hundreds of delinquent transactions when each has a different reason for being incorrect. The 100% interrogation approach may be best used before an audit is carried out to help decide which areas should be subject to audit cover.

The 100% interrogations do have an important role in audit. The section on information systems auditing will argue that the auditor should have a suite of downloaded databases for each main computer system. These data should be examined through special audit tests looking for possible fraud and error. These limited 'reviews' have a role in the audit plans and can be used to uncover much material that can be reported to management, or form the basis for further audit work. This cannot replace the all-consuming systems-based audits that should be the bulk of audit work. Within the context of systems auditing, 100% interrogations provide a powerful tool for discovering the condition of the data and commenting on the state of controls. This is less significant for systems that are not primarily there to process transactions, but have a service delivery profile. It is still important that all underlying information processes are correct and proper. Testing can prove this point so long as it is put into perspective. Returning to the audit of pensions, we can test the database to establish whether our concerns about information system controls are really operating. Our audit is not a series of interrogations of information systems but a considered opinion on the adequacy and effectiveness of managerial systems of risk management and control.

The Meaning of Compliance

Compliance testing seeks to establish the degree to which control mechanisms are being applied as prescribed and the results should highlight non-compliance in pursuit of the defined test objective. Often what is meant to happen does not, and procedures that should be in place are ignored. An extreme example of the importance of independently confirming the operation of procedures at a care home for the elderly comes from the work of an investigative journalist:

> Our reporter was given a job after a five-minute interview in which he explained that he had no relevant experience or qualifications. He provided false references and a fake CV. The management failed to follow up his reference or check his CV. He was given no training but, within hours of arriving at the home to start work, he was asked to look after frail women patients. The investigation centred on a home in Birmingham, but what Chris Millar uncovered will deeply concern anyone with a relative in a nursing home or those about to consider such a move . . . Elsie, in her 70s, was imprisoned in a chair for hours . . . helpless elderly residents were left covered in excrement – not surprisingly one dazed old man told me: 'I wish I was dead'.[8]

The simple concept of compliance testing actually involves a number of interesting questions:

What is the definition of compliance? The starting place for a compliance check is the precise definition of what one is seeking to conform to. When considering whether a control is in use, we must decide the model of control adopted. Where management believes that a key control is being applied, say use of unique and individual passwords, this should be subject to a further check before we can say it is an effective control. Passwords along with user IDs allow management to restrict access and know which people have interfaced with the system. Where these passwords are swapped at will, the control fails and we must have knowledge of this before we can determine the detailed test programme. Compliance testing then comes into the frame to decide whether parts of the operation should be subject to substantive tests as a prerequisite to forming an opinion.

Why do people not comply? Compliance testing programmes will determine whether something is being done. The results will be used to help the auditor decide whether controls are adequate, by highlighting the improper use of what should be accepted procedure. What it cannot say is why certain operations that constitute controls are not being adopted. The auditor is charged with placing the results into context by understanding the reasons why matters are not as they should be. Where procedures are not being followed we may take a step back and suggest that the same procedures should be assessed for adequacy before we tackle the subject of adherence. Where they do not make sense or are out of date, there is little progress in stating that there is breach of procedure. We need to provide management with insight into what is going on. One question is whether it is necessary to comply at all and this is covered below on compensating controls.

Can controls be compensated for? There are times where controls fall out of date or become inappropriate as the system adapts to its environment. Front-line controls fall out of place and back-up controls appear as staff seek to ensure that the operations work. We find staff deal with problems by establishing another level of control to fill in for any perceived gaps. A system for car mileage claims may state that managers should certify claims before they are paid as a key control. Where this task is not taken seriously, we may find payroll staff querying the claims where they are obviously inconsistent. This check by payroll acts as a compensatory control that may not appear in the official procedure in line with the principle that people generally want good controls. Systems of internal control operate together and where one part is weak (i.e. not adhered to) another part may well take over. Auditors may need to look for these compensating controls. They will need to decide whether to recommend that management adopts them as official procedures on the basis that they reflect the shifts in control balance that occur over time. Most compensating controls depend on a good control culture, which means that an organic view of procedures is adopted to a better effect. We cannot always take extra procedures as being the most efficient method, as they may not be based on an overview of the entire operation and

interfaces. The auditor must test compliance with official controls and apply the same tests to compensatory ones.

Issues in Testing

1. The fraud investigation perspective The increasingly high profile that internal audit has assumed in fraud investigations has to meet the requirements of the 'expectation gap' that calls for these types of services. We all appreciate that management is responsible for the prevention, detection and investigation of fraud and irregularity, although we also know that this role is shared with (if not given to) the auditor. The link between the auditor and a profile in fraud investigations apart from the control implication is the way testing can be applied to this type of work. This enables the auditor to research problems in a way that managers are unable to, in the search for the offender. Managers when confronted with a fraud tend to want to confront the alleged offender and 'have it out', while the auditor will tend to stand back and develop a series of test programmes to secure evidence concerning the fraud. Herein lies the main difference where auditors possess techniques that enable them to probe, examine and review material relevant to the case in question. We have mentioned various methods for securing relevant information and these are likewise applied to fraud investigations albeit with a different objective in mind. The key difference between a systems audit and a fraud investigation is the emphasis on purist testing routines that are applied to the latter work.

2. Substantive testing and the 'expert' dilemma The concept of substantive testing must be dealt with carefully. During substantive testing we establish whether a business objective is being achieved. This requires a considered judgement on whether something produces the right result. Questions such as 'is this right? does it make sense? is it correct? is it proper? does it work?' all substantiate the true position. The application of substantive tests to traditional financial systems is easier since the control objective will be concerned with the value, timing and presentation of figures reported by the system, which may be measured. Where we tackle managerial and operational areas we turn to qualitative considerations that are more difficult to measure. These may relate to the impact of services on clients and VFM that require the auditor to substantiate whether controls produce the desired effect. Expanding the concept of effectiveness brings with it even more demands as this is difficult to quantify. The conflict between the need to directly substantiate something and provide a considered judgement can lead to problems for the auditor. This is where a substantive test depends on an interpretation of the results of the applied test procedure. These complications add spice to the audit task.

3. Do we need to mistrust everyone and everything? Testing applies the principle of asking what, where, when and why, which is ingrained into the auditor as part of training and experience. We commend the auditor who probes, and we recognize the need to examine in detail transactions from all systems. These skills are applied with great determination since we must test as much as possible and complete the test programme. The premise of this derives from mistrust of people and documents. We seek evidence from as independent a source as possible in line with the audit objective. There are implications of a position where we do not trust anything until confirmed. The way this potentially confrontational position is managed takes care and practice. Meeting with management the auditor requests many documents referred to in discussions. When managers say they wrote to staff on data protection, we ask to see the memorandum. When managers argue they sign all orders before dispatch, we examine

a batch of them. The auditor verifies representations, although comments may be reported accurately: 'management has indicated that . . . ' or 'we were informed that . . . '. We should ask for confirmation in a way that does not imply mistrust but falls under standard auditing procedures. The best approach to explain this procedure to management is to depersonalize it.

Reliance on the Work of Others

We can turn to an older IIA.UK&Ireland's Professional Briefing Note (Ten), Working with Other Review Agencies 1996, for a considered view on the extent to which reliance can be placed on the work on others. Selected extracts follow:

- In order to improve audit's efficiency and minimise duplication of effort the auditor should where possible use the work of other auditors and review agencies where it can be relied on. Furthermore auditors may encounter a specialist, professional or technical area in which they are not experts and need to consider and make use of expert opinion. (para. 5.1)
- In its extreme form, using the work of another reviewer may be viewed as an alternative way of obtaining audit evidence. A weaker form is when the auditor makes use of the general findings and conclusions of another review agency in planning and risk assessing or as a factor in assessing the strength of control. (para. 5.2)
- The position of the internal auditor is different from that of other review agencies in that the auditor may evaluate the review agency itself as well as assessing the extent to which it can place reliance on specific work of the agency. (para. 5.3)
- Specific guidance exists regarding the relationship between external auditors and others. It is helpful to examine this guidance because the principles relating to the concerns of the auditor of financial statements are also relevant to the internal auditor. (para. 5.4)
- The auditor needs to consider the substance of any evidence provided by the other agency, the sources of data, assumptions made and the effect the evidence has on the audit. The auditor should have the same confidence in the evidence derived from the other agency as if it had been obtained directly. (para. 5.7)
- An auditor may make use of an expert opinion where the auditor does not have the experience or knowledge to be able to form an opinion on a technical matter. In these circumstances the auditor should confirm that the expert is appropriately qualified and expert in the relevant field and was independent and objective in examining the facts and forming an opinion. The expert opinion may then be taken into account as part of the evidence used in forming the auditor's own conclusions. If appropriate the auditor should indicate the extent to which the expert opinion has been a significant factor. (para. 5.8)

Computer interrogation is a powerful technique that can be applied to audit testing and is mentioned in Chapter 7 on audit approaches. However, we need to think about interrogation as a front-line audit technique and not a specialist tool. Richard Todd has prepared a paper for the Handbook that supports the widespread use of automated interrogation.

Computer Assisted Audit Techniques – Richard Todd

Introduction

Audit testing is the main source from which audit findings will emanate; in many respects this is perhaps the most time-consuming area of audit work, in that it relies heavily on the help

and assistance afforded to the auditor by the audit client. Testing is the process of examining and evaluating transaction vouching and verifying transactions in order to establish whether such transactions meet given criteria. Given the tight budgets surrounding the audit process nowadays the auditor is under ever-increasing pressure to produce a good quality audit product in a timely fashion. In practice this means producing a comprehensive audit report in line with the terms of reference and within budget. A lot of data nowadays are held on computer systems in one form or another. In fact you would be hard pushed to find systems that don't use computers. With the cost of computer hardware and software reducing, and with the onward step of information technology, in almost linear progression, computer systems have become a way of business life. The systems-based audit philosophy has been driven in part by bigger and more diverse computer systems with hoards of data. An auditor can only hope to test a small proportion of data when faced with such systems. For example, a relatively small debtor system could hold 100,000 records, an auditor may only have 10 days to review the system. The question is how many records would he test, or how many could he test? The answer is really not very many in relation to the whole amount. Computer Assisted Audit Techniques (CAAT) is an approach that uses a computer to conduct the testing. Taking this a stage further, what if one could test all 100,000 records against a given control objective, why then bother with a systems-based approach. In my view a systems-based approach can be complemented by the use of CAAT and the two are not diametrically opposed. One important thing to remember when I speak in terms of CAAT is that I am not talking about computer audit per se, as I do not see the use of CAAT as the exclusive right of the information systems (IS) auditor.

Example of the use of CAATs

A computer generated debtors report states that there are 100,000 debtor records culminating in an overall debt of £5,000,000. The test objective is to confirm that the overall debt is fully supported by the individual records held on the system. A general approach would be to select a sample and check that the individual debt on a given records was included in the overall debt. How many records would you check in this way – 250 perhaps, the result of which one would then extrapolate to represent the total sample population. The CAATs approach would be to recalculate the whole, by taking every record (100,000) and completely adding the debt from each record, the summation of which would be the total debt. The auditor would then compare the CAATs total with the system generated report total; the two should be the same. If there were a discrepancy the auditor would then be entitled to raise questions over the integrity of the systems reports. This is only one type of example of how CAATS can be used – other uses include: data matching, data stratifying, data reconciliation and data omission. Data matching has become big business in particular with regard to investigating fraud. The matching of common fields on two separate databases has now become a common investigative tool. In one organization that I worked for, management felt it was unacceptable for staff working for the organization to owe money to the organization. A management instruction was issued to all staff outlining management policy on this issue. A few months later management conducted a data matching exercise the test objective being to confirm that no staff members had outstanding debt with the organization. The payroll system's bank record details were matched with the debts system's bank details. The ideal situation would be that there were no matches; the real world situation was that there were some matches, which led to further enquires and in some cases subsequent disciplinary action. Other areas included looking for duplicate transactions, i.e. an invoice paid twice or an individual on the payroll twice. In one audit that I undertook of a devolved creditors system, the client

was concerned about the possibility of duplicate creditor references on the file and thus the real possibility of duplicate payments. One would hope that the systems controls would prevent such a situation occurring. The reality sometimes is quite different. Some organizations are so big that there is a possibility that they can invoice a client twice from separate sources for the same service, in so doing invoice details are different but the amount is the same. A CAATs approach to this would be to match the same amounts paid to the same credit reference in the period under consideration, and also to match creditor names against creditor reference numbers. The test objective is to confirm that all creditors have only the one credit reference number and where two payments of the same amount were paid to the same credit reference number that such payments are bona fide.

I once had the privilege of working with an IS auditor who walked around with a laptop and data transmission cable and for every audit he undertook he went for the jugular (the data). He would always as a matter of routine ask the client for the data for which they were responsible. There was no electronic systems data that he could not access. He would then take the data and manipulate them looking for idiosyncrasies; when he found anything of note he would seek explanation from the client. This was a very important time in my career as it helped to change my perception and thinking with regard to data accessibility. When I conduct a review nowadays, I always try to obtain the system's data, or a segment of data, which could be a zone, group or neighbourhood, inter alia. The auditor can see any one segment of data as a microcosm of the whole state of the database, and therefore any results will be a mirror image of the whole database, all other things remaining equal. Needless to say clients feel very uncomfortable when handing over data, their comfort zone is eroded, for data do not speak with forked tongues, they tell the whole truth and nothing but the truth in terms of what is on the system. Whether that which is on the system is correct is another matter entirely. Where anomalies are identified on the system the next audit issue is to look at the control weakness which allowed the anomalies to exist in the first place. The client, when faced with hard evidence, tends to respect the integrity of the auditor more in that the auditor is asking pertinent questions about data rather than general questions about systems. Waffle and speculation can no longer help the client when confronted with data irregularity or inconsistency. Sometimes it's simple operational matters that the auditor uncovers such as poorly formatted address fields, or other areas of information that have not been consistently captured in a standard manner. The next logical question to the client would be: Are there documented procedures for the formatting and data entry of address fields. If the client answers in the affirmative then it suggests that procedures are not being adhered to. However, as the situation unfolds the auditor is in the driving seat, and I for one would sooner be driving than on the client's bonnet, so to speak. The client will be more inclined therefore to accept the findings and thus the recommendation if they are supported by CAATs.

Problem with CAATs

Many audit departments still regard the use of CAATs as the preserve of the IS Audit, other auditors who want to venture into this area usually have to do so via the IS auditor. Such a view is narrow and only serves to weaken the audit department as a control entity within itself. Another problem that sometimes impedes the use of CAATs is audit budgets. Very often, if an auditor has limited time constraints, the last thing he/she might want to do is apply a CAATs solution to an audit problem. The drive for enhanced use of CAATs techniques must emanate from audit management, in other words management must have the vision of where and when the possible use of CAATs techniques are appropriate. The other stumbling block is a lack of

training of auditors to do the job. Good training is expensive and tight audit training budgets don't always allow for it. The most difficult problem in my experience of using CAATs is importing data. If any CAATs system is to work effectively one must be able to import the data in a format that the system will read. The auditor mostly knows exactly what information he/she wants and in what format, although the CAATs systems are now becoming more sophisticated and are able to identify different formats and automatically convert them. The auditor must, however, be mindful of the need to capture data in a complete and controlled manner. Remember any data corrupted or lost in the data transmission process will render the test incomplete and therefore cast doubt on the test results. Over the past few years I have worked in several internal audit departments, and in that time I have only observed one general auditor attempt to use a CAATs approach to an audit review; and because it was not fully supported by management it was fraught with technical problems. Using a computer assisted audit technique does not mean one has to necessarily use an audit package, rather it is possible to use a spreadsheet package (Microsoft Excel) with the advantage being the reduction in the cost of purchase of the package and training. If a spreadsheet package can perform a good CAAT function it can be used to check, stratify, match records and identify trends and there is no reason why it should not be used by auditors as an computer audit tool. It is the mindset of the auditor that is key and accessing the data offline in an environment where the data can be manipulated.

Future of CAATs

Auditors are under increasing pressure, whether internal or external, to deliver better quality services. In the beginning there were 'tick and check' audits where the auditor had a green pen and ticked transactions as he/she tested them. Then there was a systems-based audit, which moved away from 'tick and check' and looked at the key controls surrounding the system. The 'tick and check' approach was then relegated to the realms of history and is only now used on investigations where detailed checking is required. With the arrival of cheap computer hardware and the extensive use of computer systems we now have CAATs. What we don't yet have is extensive use of CAATs by generalist auditors. In the old days we, as auditors, would take the books of account from the client in order to audit them. Why then because it's in electronic format would we not take the data in the same way now? The principles have not changed, it's the practices that should change in line with the times. Auditors must be able to improve the quality of the service at all times if they are to maintain and strengthen their role within organizations. It is worth remembering that a strong internal audit department is a strong control mechanism and this will enhance and improve the organization's long-term standing. This is particularly poignant given the recent scandals within large companies. An audit department, which conducts routine systems reviews year on year without applying CAATs, is effectively putting all their eggs in one basket. Auditors themselves must think data. Once you have good data and you know how to manipulate them you can apply that skill routinely across any database. The essence of the 'Big Brother' society that we all now live in is based in principle on CAATs or its equivalent to conduct data matching, so whether we like it or not it's here, and as auditors we had better get with it. Auditors who fail to embrace new techniques will in future find themselves surplus to requirements, as younger auditors who know very little of the past will embrace new technological skills as second nature. The quality of the audit product is what will provide longevity for the auditor while elevating the audit service within the organization in which the service operates.

9.6 Evidence and Working Papers

Audit testing results in much material that should support the reported audit opinion and associated recommendations. The test results along with other material gathered throughout the audit process will constitute audit evidence and this will be held in suitable audit working papers. Standards of working papers and documentary evidence are a topic that all auditors come across in the course of their work and generally there is a view that good standards are a prerequisite to good control. Practice Advisory 2330-1 covers documenting information, based on standard 2330:

> Internal auditors prepare working papers. Working papers document the information obtained, the analyses made, and the support for the conclusions and engagement results. Internal audit management reviews the prepared working papers.
>
> Engagement working papers generally:
>
> - Aid in the planning, performance, and review of engagements.
> - Provide the principal support for engagement results.
> - Document whether engagement objectives were achieved.
> - Support the accuracy and completeness of the work performed.
> - Provide a basis for the internal audit activity's quality assurance and improvement program.
> - Facilitate third-party reviews.
>
> 3. The organization, design, and content of engagement working papers depend on the engagement's nature and objectives and the organization's needs. Engagement working papers document all aspects of the engagement process from planning to communicating results. The internal audit activity determines the media used to document and store working papers. The chief audit executive establishes working paper policies for the various types of engagements performed. Standardized engagement working papers, such as questionnaires and audit programs, may improve the engagement's efficiency and facilitate the delegation of engagement work. Engagement working papers may be categorized as permanent or carry-forward engagement files that contain information of continuing importance.

Note that the external auditor may be sued where their work may have been performed negligently and their working papers may be used in any defence to this charge. Here we look at some of the requirements for internal auditors' working papers and filing systems.

Evidence Attributes

The evidence the auditor uses for the audit opinion should be:

Sufficient This is in line with materiality, level of risk and the level of auditors' knowledge of the operation. Sufficient means enough, which depends on circumstances. It should be enough to satisfy the auditor's judgement or persuade management to make any changes advocated by audit. It could mean enough to ensure that there is a wide spread of material or an acceptable sample. Evidence is adequate when it meets the desired purpose. The audit opinion may range from 'it is clear that . . . ', 'it would appear that . . . ', 'there are indications that . . . ' and 'there is the possibility that . . . '. In the current environment of cost constraint, the amount of evidence secured should be the minimum to form an opinion in that it takes more resources to obtain relevant proof that conclusions are sound.

Relevant This ensures that evidence is directed to the control objectives. Relevance brings into play the legal concept of admissibility, which requires material to relate specifically to the issues at hand. It is wrong to refer to matters that do not impact on the arguments that appear in the audit report, as a way of blurring the issues at hand. The auditor must use professional judgement in deciding what is important. Test results that refer to low-level detail cannot be used to comment on material considerations that have a far-reaching effect on management's ability to achieve. Relevance means that the evidence is associated to the key concerns and that it is material to them.

Reliable The information should be accurate, without bias and if possible produced by a third party or obtained directly by the auditor. The term 'reliable' stimulates images of the evidence being 'dependable, honest, sound and true'. This may in turn be applied to the audit report that is based on this evidence, as in one sense and in contrast, unreliable evidence creates an opposite impact by lowering the credibility of the auditor's work. The rules on obtaining audit evidence require it to be done in a way that minimizes bias. The reliability factor must be applied by the auditor to satisfy him/herself and must also satisfy the perceptions of the report reader. Independence and accuracy are the main components of the reliability index that need to be fully addressed by the auditor, in the search for good evidence.

Practical One would weigh up the evidence required, the cost and time taken to obtain it and sensitivity. Some matters cannot be discovered through audit since it would take too much research. There are many examples of this that range from getting a definitive verdict on the state of the MIS database, through to obtaining a view on whether staff are well motivated. Not all matters may be studied and documented by the auditor since the general equation suggests that the greater the value of evidence the more resources will be applied to securing it. There is a constraint that means there is a strict limit on the time that can be applied. The IIA Performance Standard 2300 makes it clear that: 'Internal auditors must identify, analyze, evaluate, and document sufficient information to achieve the engagement's objectives'.

Types of Evidence

Material to support audit findings from testing would include:

- Documents
- Analysis of figures
- Third-party confirmation
- Vouching checks
- Testimonials
- Interview records
- Re-performance by audit
- Reconciliations
- Reports
- Verification
- Physical material, e.g. photographs

Working Papers

Test results will be contained in working papers held in audit files. Working papers should:

Set out the objectives of the work The entire documentation is prepared or secured for a reason and this reason should be defined at the outset. The reason the work was carried out that resulted in the relevant working paper should be stated in a way that sets a firm context for the interpretation of the information contained therein. This will help indicate the extent to which the document being relied on by the auditor fulfills the overall audit objectives.

Show clarity The working papers should be laid out clearly to promote their use during report writing and review of work. Papers should be set out in a neat and orderly fashion that is logical and simple. This is aided where documents contain a list of abbreviations used and definitions of any common terminology and keys. One well-known test is that if one found a sheet of paper from any working paper file, it should be immediately identifiable.

Be indexed The first enclosure of any file should always consist of an index to the papers. This should indicate where documents can be found and what each one contains. It is better to start the index sequence from the back of the file so that newer documents can be added.

Support the audit decisions/opinion Working papers are secured primarily to ensure that audit findings can be justified. Cross-referencing should be applied whereby the report held on file contains references (in the margin) that relate to specific enclosures held in the working paper file. Figures, examples, quotations and charts should be able to be traced back straight to the file. This is particularly relevant where the report is contentious. Working papers are used at pre-report drafting stage where findings are being discussed with management.

Use pro formas One way to promote the use of audit standards in working papers is to use standardized documents. These act as checklists, forcing the auditor to cover specified areas during the course of completing the required document and also form an *aide mémoire* in guiding the auditor. The documents may be used as pure evidence where material is extracted from source records and then input onto the form. Alternatively they may be used to summarize the material from records and analysis that is attached to the pro forma. One further advantage is that they appear tidier as an alternative to reams of rough hand-written notes. Automated working papers come a step closer where we are used to working with standardized documentation.

Be cross-referenced Working papers form a whole in that together they tell the story of the audit in terms of work carried out and resultant findings. In an audit each stage leads naturally to the next. Findings from one piece of research will impact on work done on other areas as the flow and direction of the audit changes with new findings. These links and associations should be reflected in the working papers by a suitable system for cross-referencing. The file should be capable of being read in parts as well as an entire audit document and if a file were to be reconsidered months (or even years) after the audit is completed, its contents should still be crystal clear.

Be economically used Working papers contain evidence and material relating to the audit. The papers should not be prepared for their own sake but must relate to specific audit objectives. If we flowchart a system, this should be left out where, due to circumstances, it is not required. Filling files with superfluous material will blur the real issues and lead to inefficient use of audit time.

Be headed up All documents should contain headers with the name of the audit, date, relevant officers and other details. Any document prepared by the internal audit unit should be able to be identified by the headings.

Clearly show any impact on the audit report Some documents have a profound impact on the audit report while others provide background. The status of working papers should be clear in that items that feature in the report should be indicated. A scan of the working papers

should give an idea of what points will appear. One way of providing this standard is to highlight (by a coloured pen or font) sections that will enter into the report to create this distinction. A brief review of the working paper file will isolate the key material without having to re-read all the contents of the file.

Be signed by the auditor and the reviewer It is practice to place at the bottom of each document, boxes for 'prepared by' and 'reviewed by' along with spaces for the dates. This underpins an audit standard that dictates that all evidence indicate the preparer. It encourages the audit manager or senior auditor to record that they have reviewed the document in line with QA standards.

Show the work carried out Documents support the audit opinion and contain matters that may be referred to in the audit report. While this gives a bottom-line use for the working papers it is equally important that the underlying work completed be fully identified. This sets a context for the conclusions that may be important at a later date. Factors relating to the way source evidence was examined and recorded should be documented as a formal account of the procedures. If missing there is a temptation to leave out controversial material not derived from fully understood procedures.

Show the source of information/data The origins of information in working papers should be clearly defined. Where the data were obtained from filing systems or computerized databases, the date and circumstances must be recorded, since the same data may be altered at a later date. Where an officer has made a representation that falls within the working papers, the source should be noted, particularly where it relates to specific figures.

Indicate which matters are outstanding A working paper will say what has been done and the results of this work. For the record it should make clear what work has not been undertaken as this may arise as an issue. Where parts of the system have not been addressed this should be made clear, particularly where a different level of work would have been required. Where samples have not been fully tested because of various practical difficulties this point should appear on the working paper to explain why certain items have no results listed against them. Examples may cover many different areas, although the basic principle is simple in that qualifying information is just as important as positive findings in terms of providing an acceptable foundation for the report.

Show any impact on the next audit The working paper indicates what has been left for later consideration. The nature of audit work means that not all matters are addressed in any one operation and two audits can be carried out in the same area dealing with different aspects. It is helpful if files show where future resources may be concentrated in terms of covering gaps left from an earlier audit. This should 'jump out' from the working files to feed directly into the next audit of the area.

Be complete There is nothing more frustrating than reviewing a file that suggests that certain items have been missed for no apparent reason. Files should be complete, in that all they purport to cover is dealt with. For standardized documents this is particularly relevant since where a predetermined item is not deemed necessary it must be noted as 'not applicable' with suitable explanation.

Be consistent Working papers should be wholly consistent. This is important where the audit has been done over a long time period and/or involves several auditors, each dealing with a different part. If a figure or fact is quoted in one document, this should be the same as in another or differences explained. This rule also applies to statements and representation made during the audit and recorded in the working paper files. Where this does not occur and there are inconsistent facts then the normal option will be to exclude all reference, because of uncertainty and thus lowering impact of the report. Any audit manager's review of the working papers must seek to identify inconsistencies between the working papers and the draft audit report.

Include summaries wherever possible It is one thing to obtain and file vast volumes of reports, printouts and documentation in that they impact on the audit. What is more important is to digest, analyse, and then summarize the material components of this information so as to avoid re-reading bulky material. So a consultant's report on an operation should be read by the auditor and then key points extracted and summarized. The consultant's report should not lie in the file without comment. Likewise extensive test results should not appear in spreadsheets without bottom-line conclusion that can go straight into the audit report. Detailed figures are meaningless if no conclusions can be drawn. Larry Hubbard has provided some useful advice on compiling working papers:

> One of the most important functions of organized audit workpapers is that they give auditors a place to put information during the audit. The words 'during the audit' should be emphasized because many times I've seen that workpapers were compiled after the audit ended, rather than as it progressed. What a waste! Building workpaper binders as you audit enables your documentation to contribute to the value of the audit. Data is organized, and the risk of losing items is reduced; plus, if the auditor wins the lottery and doesn't finish the job, others will have an easier time locating the necessary information to complete the assignment.[9]

Permanent Files

These files contain standing information of a permanent nature such as:

1. **Organization chart.** This shows names, designations and position of staff. It will fall out of date but indicates structure. Management may provide updates.
2. **Risk register.** Corporate and business risk registers should have been compiled by all relevant parts of the organization where risk management systems have been established.
3. **System notes.** Notes and flowcharts from previous audits that document the movement of information and documentation should be held on file so that a good picture of the operations is secured in the permanent files. Again these will tend to fall out of date as changes arise.
4. **Research items and relevant publications.** Publications that relate to the operation will help provide an overview of current developments and keep the auditor in touch with the changing factors that impact on the particular work area. Bulky material may be held in the audit library and simply referred to in the permanent file.
5. **Summaries of frauds.** It is good practice to link fraud and irregularity to the systems work as a way of seeking improvements in controls that allow problems to arise in the first place. A reference to frauds that impact on the operation will assist.
6. **Management reports.** Reports prepared by consultants and management themselves should also be obtained and held on file or appropriately cross-referenced. This is a good

way of keeping in touch with matters that are of concern to management without performing an actual audit.

7. **Committee papers.** Reports that are submitted to committee (or the board) for approval usually involve new acquisitions or restructuring exercises. Relating these to the permanent files adds important knowledge concerning proposed and approved changes that may have a control implication.
8. **Budgets and other financial data.** Financial reports can be used to assess materiality. They can be further analysed to obtain a view of changes in spending patterns of interest to the auditor in planning future work. Permanent files have two main uses in that they help in setting long-term audit plans (via risk appraisal) and also provide background information.
9. **Previous audit reports.** The executive summary of previous audit reports should be held on file as each report should ideally run only to a few key pages. This is in addition to references to the full audit report that should be filed elsewhere.
10. **List of premises and addresses.** Useful information such as brief maps and transportation arrangements for each site can be of great aid to the auditor. We would also require a list of contact names and phone numbers. This will involve employees who have in the past been assigned to assist the auditor and recognizes the protocol that is sometimes applied by management where they nominate specific link officers for the audit.

We would wish to retain in our permanent files, information of continuing relevance to the area in question so long as it is material to the audit objective. Armed with this we would want to derive a risk profile of each main operational area for planning purposes and as a way of developing a database of relevant information concerning key parts of the audit field. It would probably be advisable to assign specific parts of the audit field to auditors for continual updating and amendment. In addition, close liaison with management should ensure that all relevant materials are entered into the filing system. The updating process should also require the auditor to assess the impact of new information as it is placed on file. This may act as a funnel mechanism where all relevant information ends up in the correct place within the filing system.

Current Files

These files record the results of the audit assignment. They contain items such as:

1. **The objectives statement.** The first document that we might come across may be a statement of audit objectives that sets the tone for the resultant audit.
2. **The preliminary survey and risk assessment (risk registers).** In the section on audit planning we have agreed that assignment planning starts with a preliminary survey where key risk areas are identified for proposed cover. The work done in this respect should be fully recorded on the current file.
3. **The scope of the audit.** Having completed the preliminary survey we may now define the scope of work in a formal document. This will be in two forms. One will be a file document that is agreed to by the audit manager. The other will be a memorandum to the auditee advising on the scope of work that will be carried out in discharge of the audit objective. Both documents should be held on the current file.
4. **The assignment plan.** The work undertaken to prepare the assignment plan should be properly recorded on the current file. This will be used to set a frame against which the actual results can be measured and as such constitutes a major control over the audit process. The

planning schedules will be updated as details of actual audit hours worked are made available. The documentation should also include an administrative schedule that sets out clearly who is responsible for what parts of the audit.

5. **The results of any background research carried out.** Interviews with staff and management should be fully recorded and held on file. These are important for later use as we may have to quote from representations made by management. Also a review of the working paper file will make it clear whether management has agreed that there are certain weaknesses and we may have made notes on the response to resolving them that can be reported on. It is best to hold interview notes in plastic pockets so that any documents referred to during the interview can be placed next to the interview notes themselves. It may be that something said by an officer conflicts with other views from auditees and it is as well to know which material was provided by which person.
6. **Systems notes and flowcharts.** These are obviously important file documents. The interesting point for these papers is that they will probably need to be copied and held also on the permanent file since they will have a continuing relevance to the audit unit in question.
7. **Any audit programme used.** Programmes come in two forms. Some list the tasks that need to be completed to perform the audit, while others contain space to record the results of the work carried out. Whatever the format, they are essential material for the current file as they feed directly into the audit reporting process. It is good practice to highlight those matters that will be used as examples of the implications of poor control of risks, when the report is prepared. The format of the schedules should be carefully considered. It is one thing to list errors and concerns and quite another to have them ordered in such a way as to allow summary figures to be reported. So, for example, where we wish to report on the percentage of items exhibiting a particular type of problem the working papers should accommodate this requirement by allowing composite figures to be readily extracted.
8. **The system evaluation.** Much of the audit opinion is inferred from the evaluation of controls in terms of defining weaknesses that are then reported on. Some systems audits pay little attention to the evaluation stage and the working papers reflect this approach by not containing a great detail of control assessment. Notwithstanding this, the formal evaluation documentation, be it by ICQ or control evaluation schedules, should be held in the current file as a record of this process.
9. **The testing strategy.** Test programmes indicate what will be done as well as by default defining what will not be covered. Formal documentation on the current file is required as part of the working paper standards applied to current files. It is one thing to list the great lengths the auditor has gone to in performing testing and the detailed results that will probably be recorded. However, the process of deciding what to test and how it is sometimes lost among the vast amount of material that testing tends to produce. This factor can be very important at a later stage where, for example, a fraud occurs shortly after an audit has been completed having disclosed no material concerns. The way samples were selected and dealt with can be an important point where there is some dispute over the audit work. Again this initial strategy should be clearly set in the current file so that conclusions concerning this stage of the audit can be readily extracted.
10. **The test results.** We now arrive at the actual testing stage and this will normally produce material that will be referred to throughout the audit. The need to have this evidence recorded in a clear and accurate manner cannot be overemphasized.
11. **Internal control evaluation schedules.** This document should set out the control objectives, initial assessment of control mechanisms, the test results, the opinion and recommendations. It will form the basis of the closure meeting with line management as

the key points are discussed in some detail. We should end up with an initial management response that can also be entered onto the record of control weakness. Many of the matters set out in the record will enter directly into the draft report, and herein lies another reason why the document should be carefully drafted and held on the current file.

12. **The audit report.** A version of the audit report that contains direct references to the underlying working papers should also be held on the current file. We should make sure that this is the same version as the final issued report, as we would expect several drafts to be prepared and revised during the course of a typical audit.
13. **Audit review notes.** The current file should contain a formal audit review record that should indicate what checks were made by the audit manager in question and that the audit meets quality standards. The main problem is where the review is not formally documented in the file. A further problem is where the audit manager has reviewed a draft report that ends up with many comments written on the report pages. The draft may then be destroyed as new versions are prepared and review points then lost. As such it is important that the audit manager details the review points (say concerning the draft report) and that this is held permanently on file, even if the draft report is destroyed. To expand this point it may also be advisable to record significant meetings between audit management and the lead auditor where the audit is discussed.

Linking Permanent and Current Files

There is an obvious link between the permanent and current files as much of the material of continuing importance collected during the audit will end up in the permanent filing system as shown in Figure 9.17.

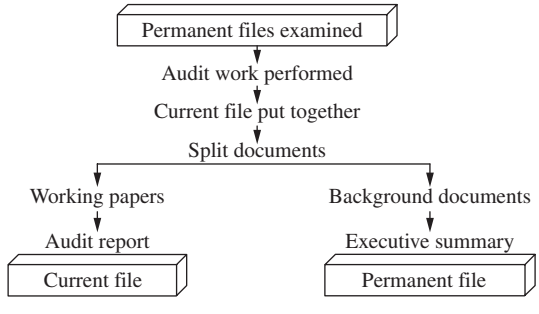


FIGURE 9.17 Permanent/current files linkages.

Standardization

One way to formalize the process in Figure 9.17 is to define standardized working papers aimed at getting to the audit opinion with supporting evidence. The IIA's Practice Advisory 2330-1 (Recording Information) suggests that: 'The CAE should establish working paper policies for the various types of engagements performed. Standardized engagement working papers such as questionnaire and audit programs may improve the efficiency of an engagement and facilitate the delegation of engagement work'. These standardized documents will form the current file while the background material will either be held as a bundle of general papers or, if relevant, will enter into the permanent filing system. This approach forms the basis for an automated filing system

where standardized forms are maintained on disk. Standardized documentation enables auditors to follow a systematic audit methodology and can contribute to overall audit efficiency. This point is explored later in the section on the audit manual. These are certain types of documents that might be standardized including:

- Preliminary survey report
- Flowcharts
- Internal control evaluation forms
- Record of control weakness
- Constraint analysis
- Assignment plans
- Interview records
- Compliance and substantive test strategies
- Risk assessments
- Objectives statement

Professionalism and Working Files – Richard Todd

The following paper was prepared by Richard for the Handbook:

The audit practitioner in today's environment is facing a continuously changing profession, where time management has become central to the production of the audit product. It is a profession that has looked within itself and has responded to the need to be cost-effective, while adding value to the organization in which it operates. This is in stark contrast to the early years, where audit assignment appeared to have limitless budgets, i.e. the more the auditor uncovered the more time is afforded in the hope of further revelations. In one case I remember sitting in a motor vehicle conducting a surveillance of an employee as he travelled from establishment to establishment. My thought at the time was: what a way to earn a living. These audits were expensive and open-ended and very often inconclusive. With the outsourcing of internal audit departments came the death of the open-ended audit and the birth of fixed-time budgeted auditing. This brought about a total change in the mindset of the auditor and the professional qualities needed to discharge his/her responsibilities.

In practice, professionalism of the internal auditor is taking the 'terms of reference' of an assignment, along with budget hours allotted, and turning that into a completed audit, within time and to quality. It is common now for audits to be fixed-time, i.e. a set budget at the outset. The auditor therefore must possess certain knowledge, skills and disciplines that will aid him/her to discharge their responsibility. Coupled with this is the need for the auditor to act with a professional code of ethics. Audit budgets today are so tight that the auditor must have a definite methodology prior to the commencement of the audit, as there is so little time within the confines of the audit budget to think about anything other than the subject matter. To this end the auditor must 'hit the road running' in other words he or she must have a clear view on the end product.

When an auditor first visits an organization he must assess what type of organization it is, and what styles of audit it requires. This has nothing to do with the audit subject matter per se, rather it is an assessment of the culture and attitude of the organization and therefore gauges how such an organization will respond to audit reports. In essence this is assessing the success criteria, i.e. what the auditor will need to achieve before he or she is considered successful within the organization in question. An organization priding itself on financial excellence tends to struggle with internal audit reports, which suggest controls are not what they should be. In such a case the language of the auditor's report is key to how that report will be received. An example of this was the head teacher of a well-run, highly academic school who received an audit report which stated that certain key controls were 'weak'. The head teacher was livid; his argument was that a weak school in Ofsted terms was a failing school, and therefore should be subject to special measures or even closed down. The term 'weak' controls is standard audit jargon yet it created a

showdown. The chief internal auditor substituted the word 'inadequate' for 'weak' and the head teacher was happy.

Less well-run organizations will want and even encourage the auditor to expose systems weaknesses in an aggressive manner. The important point here is not to lose one's professional objectivity but at the same time to take stock of the client's wants and needs.

The outsourcing of internal audit services has created new challenges. Organizations providing internal audit services have to trade profitably to survive. This in itself has created a new type of internal auditor, which in turn calls for a different kind of professionalism, which includes to a larger extent marketing skills.

Some may ask how can an internal audit service can be externalized and argue that it is a contradiction within itself.

The audit working paper

Audit working papers provide the basis for audit findings and conclusions. To this end the audit file must be arranged in such a way that anyone reviewing will be able to know what the terms of reference are, what the budgeted hours are, what tests were done and what the findings are. If the audit file is unable to provide evidence of work undertaken by the auditor then the chief internal auditor will not be in a position to lend support to the audit findings. Various organizations have different audit file structures but they all essentially have the same theme, details of which are outlined below:

Terms of reference	Time management
Systems notes	Control evaluation
Test schedule	Working papers
Background	

With limited time to conduct the field work, internal audit must master the art of assembling good working papers. A well-focused audit file does help to structure the audit approach. The auditor must therefore have a clear vision of where he wants to go, and how he is going to arrive there, prior to the commencement of the audit.

Terms of reference are generally the first thing on a file. However, where preliminary background work is undertaken prior to the formulation of the audit brief then this information will also be on the file, but the detailed background information will be kept in the last section. Having established the terms of reference, the next stage will be to list contacts (audit clients) and where in the organization they might be located (organizational structure); this will form part of the systems notes. Some internal audit departments tend to confuse systems notes and working papers. Systems notes are there to document and record the system's operation, whereas working papers are a product of audit testing.

Example

Test schedules and working papers are a key element of the audit file. The test schedule sets out what the test objective is, what tests were undertaken and what the test results are. The test results must be supported by working papers. For each test there must be a working paper that supports the test results.

Detailed below is a specimen test schedule and working paper layout:

Test schedule A

Working paper W/P (a) 1
Working paper W/P (a) 2
Working paper W/P (a) 3
Working paper W/P (a) 4

Test schedule B

Working paper W/P (b) 1
Working paper W/P (b) 2
Working paper W/P (b) 3
Working paper W/P (b) 4

As can be seen from above, each test schedule is cross-referenced with a working paper. For each test result there is at least one working paper that supports it. Each test schedule is linked and cross-referenced to a control objective.

Common mistakes

One chief internal auditor once stated that the audit report was the shop window of internal audit, and that the working papers were just a means to an end, which to some degree is true.

Another chief internal auditor commented upon the quality of an audit file as being excellent despite the fact that the audit report was threadbare and lacked substance.

In some other audit sections I found that the prevailing view was: the bigger the audit file the better. The fact is none of the above is true. It is a fallacy to believe that the larger the file the better the audit. This perhaps signifies that the auditor is not clear about the scope or the extent of the field work required.

However, if an audit report is challenged, the only recourse of action is to go back to the audit file and working papers. Very often clients will challenge an audit finding. I recall one occasion where the client shouted and screamed: 'How dare you criticize me? Who are you?' He was the head for debt management. I had pointed out that much of the debt which he managed was not being pursued as rigorously as it might. In the end it came down to working papers. I had to show evidence of the basis of my findings. Once he had seen the evidence (working papers) he changed his mood and tone and became more reconciliatory.

Good practice

A block chart illustrating the flow is shown in Figure 9.18.

The working papers should be cross-referenced in such a way so that they support and demonstrate the above approach. This approach forms the basis for the report, and it allows for greater supervision, in that anyone reviewing the file can produce the draft report without having conducted the field work.

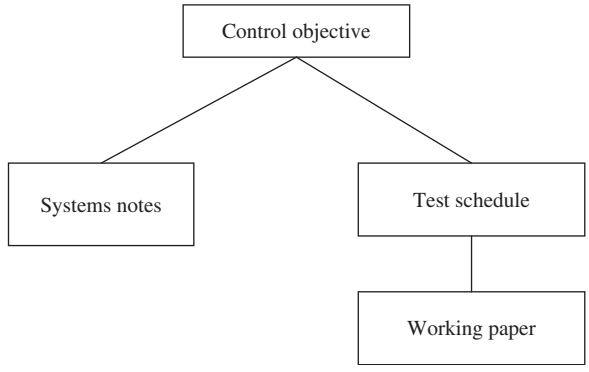


FIGURE 9.18 Audit flow.

Filing Systems

The adopted filing system should reflect the way information is stored and the different categories of files that will be compiled over the years. One might maintain the following files:

- The general risk survey (permanent files).
- File updating exercises.
- Annual reports.
- Quarterly reports.
- Final assignment reports.
- Annual plans.
- Quarterly plans.
- Audit management files including personal files.
- Correspondence files.
- Fraud allegations forms.
- Assignment working paper folders – standardized forms.
- Assignment working paper folders – background notes.

It may be possible to adopt colour coding and different file formats for all files that are not automated, for example:

1. **Orange** – General files on audit management (e.g. staffing issues), long-term plans and activity reports. General background information on the organization, its strategies and general developments.
2. **Blue** – Other permanent files, on the various systems in the audit field, broken down into defined audit units in line with the adopted audit approach.
3. **Buff** – Current audit files with standardized forms and background information on the audit.
4. **Lever arch** – Containing all general correspondence received and dealt with by internal audit that may be cross-referenced in detail to the main filing system.
5. **Lever arch** – Containing all published audit reports with a further copy held in the current audit file. Each report can be given a reference number that can be used to readily trace the document.

6. **Time monitoring systems** – This file will detail the time recording systems along with time sheets and various standardized documents used by internal audit. Moreover job codes may be cross-referenced to the numbering used in the filing system.

Each filing system will be unique and depends on the way the internal audit unit is organized. Bearing this in mind, there is one interpretation of a filing standard that is set out in Figure 9.19.

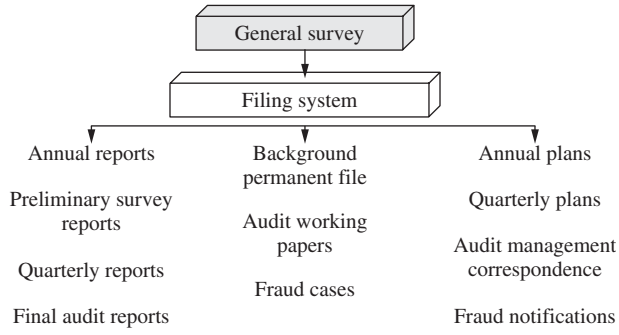


FIGURE 9.19 Format for a filing system.

The set-up in Figure 9.19 should account for most types of files and information required to manage an internal audit function, although files should be held on computer disk wherever possible. It is possible to go further and hold all these files on the audit database.

Automation

Traditional material on audit working papers deals with the attributes and standards applied to paper files. This is important since standards need to be applied regardless of the media used. Automation strategies impact on the way working papers are maintained. Most information will be on disk or accessible from corporate systems as required. Document imaging means that source documents that contain signatures and original data can be stored on disk, without manual back-up files. A half-way house is where manual files are held alongside automated files. A progressive automation programme involves destruction of paper files with information retrieval via permanent interface with computer databases. We retrieve information either on the file assigned to the audit unit or via a library system where all the material relevant to the audit unit is referenced. There is no working paper that cannot be stored on disk. We may also establish report generators that retrieve the data on the audit area. This means that the data are up to date as they are accessed from current files.

Access to Working Papers

The IIA has issued guidance on controlling engagement records and granting access to these records, extracts of which follow:

- **2330** – Documenting Information: Internal auditors must document relevant information to support the conclusions and engagement results.

- **2330.A1** – The chief audit executive must control access to engagement records. The chief audit executive must obtain the approval of senior management and/or legal counsel prior to releasing such records to external parties, as appropriate.
- **2330.A2** – The chief audit executive must develop retention requirements for engagement records, regardless of the medium in which each record is stored. These retention requirements must be consistent with the organization's guidelines and any pertinent regulatory or other requirements.
- **2330.C1** – The chief audit executive must develop policies governing the custody and retention of consulting engagement records, as well as their release to internal and external parties. These policies must be consistent with the organization's guidelines and any pertinent regulatory or other requirements.

9.7 Statistical Sampling

All auditors need knowledge of statistical sampling and it is advisable to adopt a clear policy regarding its use. We summarize popular ways statistical sampling may be applied, although a specialist textbook will provide a fuller understanding. Statistical sampling has a clear role and auditors make a decision during systems audits, as shown in Figure 9.20.

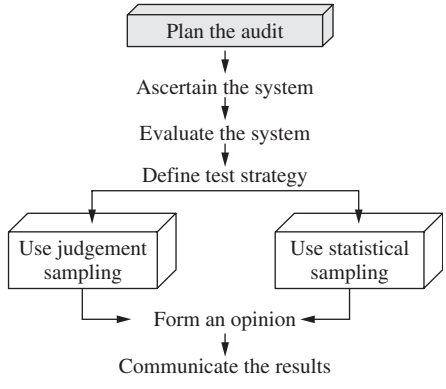


FIGURE 9.20 Role of sampling.

An auditor has to decide whether statistical sampling will be used based on knowledge and an appreciation of the technique and its application.

The External Audit Perspective

Most auditing textbooks have a chapter on sampling and so it might appear to be mandatory. One must consider the differences between the internal and external audit objectives before assessing the relative value to be derived. The external auditor is primarily concerned with:

1. whether accounts show a true and fair view. Decisions may range from disagreement, qualification, through to a level of uncertainty and as such invite a yes/no response.

2. the reliance that can be placed on underlying financial systems of internal control. As a short-cut to checking all the figures in the final accounts there may be some reliance placed on controls, although there must be some direct testing to secure evidence to support the audit opinion.
3. whether the level of errors found by examining selected transactions has a material effect on the accounts in terms of influencing the audit opinion. Materiality is a firm external audit concept that places emphasis on the impact of problems on the reliability of the final accounts.
4. whether the level of testing carried out means that they have discharged their professional responsibilities. Substantive testing is fundamental to the external audit and the need for a defendable choice is uppermost. A method to determine sample size is useful. There are tests that can be applied to 100% of a database although this gives a long list of items for further manual investigation, which will take time. The need to restrict the number of items examined remains.

The internal auditor is more concerned about:

1. whether examining selected transactions confirms initial opinion on the systems of risk management and internal control. Samples are selected and examined to see whether the results coincide with the initial audit opinion.
2. whether their findings are sufficient to convince management to act. Where management agrees that problems exist there is little point in extensive testing. It may be necessary to get an idea of the scale of the problems, although the main objective is to get management to act. The internal auditor will use a consultancy-based approach that emphasizes the solutions and not the detailed errors that fall within a test-based model. The audit report will then be based around the proposed changes.
3. whether the risk of any losses or deficiencies may be quantified. This is where statistical sampling comes to the fore. This would apply more in investigative work than in systems auditing.

In conclusion, the external auditor is primarily concerned about accepting or rejecting a financial statement while internal audit work is geared to encourage management to act on defined control weaknesses. It is the external auditor who is more concerned with the use of statistical sampling in financial audits, although it does have a role in internal audit.

Reasons why statistical sampling may not be used There are many internal auditors who do not use statistical sampling and audit departments that have no firm policy. There are many reasons why it may not be used:

1. Staff lack awareness and have had no training. This means that Figure 9.20 suggests that the auditor does not necessarily make a conscious choice between statistical and judgemental sampling because of the lack of knowledge. The fact that statistical sampling can be complicated may discourage its use. It can be time consuming to master and cumbersome to use.
2. One needs knowledge of the population and this requires time-consuming research. It may be difficult to tell exactly what is contained in the sample because of the nature of the audit. It is still advisable to analyse the populace as this gives an insight into an operation.
3. It may stifle the 'audit nose' by not allowing the auditor to be guided by years of experience. Statistical sampling relies on randomness and does not allow the auditor to choose individual transactions. The auditor's 'intuition' can be suppressed.

4. Quoting figures and probability ranges may not convince non-numeric managers to act. It depends on the perceptions of the client for the work, which vary. Some managers appreciate this approach while others feel intimidated. This factor should be balanced so as not to produce an audit report resisted by management although much depends on the terminology used by the auditor.
5. Statistical sampling is not readily applicable to small unusual populations. The real benefits come where population sizes are larger and samples relatively smaller.

Advantages of Statistical Sampling

Results may be defended against bias. Bias conjures up images of the auditor being subject to favouritism, narrow-mindedness, one-sidedness and partiality. Samples selected for no justifiable reason may foster accusations of auditor bias. Where there is a scientific method of defining sample sizes and selecting items we can assume the more appropriate stance of being objective, detached, dispassionate, fair, unemotional and, above all, just.

A defined sample size is provided. A close examination of statistical tables brings out the feature of larger populations requiring only relatively small increases in sample size to meet set parameters. A judgemental sample of, say, 5% becomes more difficult to handle for larger systems with thousands of accounts. Statistical methods permit smaller samples that are statistically valid.

One may safely extrapolate the results and apply them to the wider population. This is a moot point in that there are many auditors who extend sample results to the entire data field when the sample has not been obtained using statistical sampling. Although this prediction is usually accepted by management this is technically improper. The only professional prediction is one that sets the statistically significant results within the set parameters (e.g. 95% of cases will tend to fall within a defined range).

The technique is repeatable and one would expect a similar result from any repetition. The exercise of tossing 100 coins will tend to produce around 50% heads and 50% tails each time. With statistical sampling we would expect on average to find similar results each time the test procedure is applied.

It forces one to define and consider the attributes of the population. We set as a disadvantage the need to research the data being tested from a holistic viewpoint and this is also seen as an advantage. The more that is learnt about an area, the better will be the auditor's ability to direct the audit. Unfortunately time is now seen as the most important component of the audit function that must be controlled and this does not promote extensive pre-planning. The balance to this last point is the growing trend whereby whole databases are downloaded and explored on a regular basis. This not only encourages a greater familiarization but also allows one to generate global figures concerning the total number of records and other key facts.

Computers make statistical sampling more convenient to use. It is simple to ask the computer to generate random numbers. Many interrogation packages have in-built statistical tables.

The level of confidence may be predefined. Statistical sampling allows one to define predetermined risk parameters that the final opinion may be set within. This is factual and cannot be challenged as it states that a probable number of selections will follow a set pattern, but not all of them. This is a comfortable position for the auditor as it allows an authoritative opinion that in terms of logical presentation cannot be refuted, even if the precise interpretation may be.

Judgement, Haphazard and Statistical Sampling

Judgement sampling The auditor uses knowledge of systems and people to select items more likely to exhibit certain features. The sample is purposely biased by the auditor to take on board matters that the auditor is aware of. For example, we may be concerned about our ordering system where an individual who left some months ago was known to be medically unwell and made known errors. We may look at orders he processed and skew the sample.

Haphazard sampling This allows the selection of items at random but is not based on any defined statistical formula. The intention is to secure an unbiased sample, although because the sample size is not mathematically based, it is not possible to formally extrapolate the results. The selected sample size may be too small or too large. It is best applied to smaller populations, say under 100 items, since statistical sampling is of no use at these levels.

Statistical sampling The auditor has to define the population and set confidence levels. A predetermined sample size will be provided and one may indicate how reliable and accurate the results are. The results secured from testing the sample may be extrapolated to draw quantified conclusions about the population.

The normal distribution The bell-shaped curve represents the normal distribution. The shape of the curve is determined by the mean and the standard deviation (SD) of the underlying values whereby the greater the range of values the flatter the curve. This feature is used in statistical sampling to allow the area under the curve to equate to 1. If the mean is seen as 0 then we can calculate that each SD from the mean will cover a defined portion of the normal distribution curve. This appears in Figure 9.21.

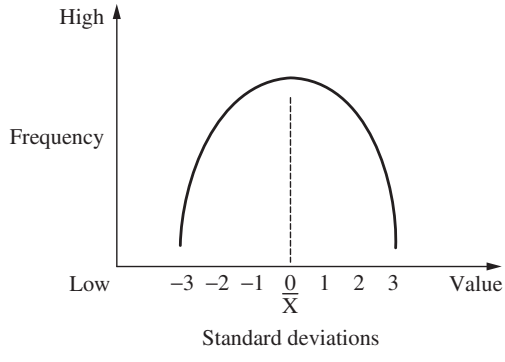


FIGURE 9.21 The normal distribution.

Area under the curve:

$$\begin{aligned} &+ \text{ or } -1 \text{ SD } = 68.3\% \\ &+ \text{ or } -2 \text{ SD } = 95.4\% \\ &+ \text{ or } -3 \text{ SD } = 99.7\% \end{aligned}$$

The relationships between the values and the SDs have been translated into statistical tables. These may be used to form conclusions about the population that are derived from an examination of a sample of the population. This is based on the theory that the mean of a distribution of sample means is equal to the mean of the population from which the sample is drawn. It is important to know the SD of the sample that is used and a formula may be used to calculate this figure. This is not reproduced here but it should be noted that the smaller the range of values the smaller the SD while the greater the range (i.e. variation from the mean) the larger the SD.

Applying Statistical Sampling to the Audit Process

It is important that statistical sampling is considered in terms of its actual role in the audit process. It is used when performing the testing routines required to confirm or otherwise the initial evaluation of internal controls. To this end the samples and ensuing tests may be used for:

Quantifying the effects of control weaknesses Substantive testing reveals the implications of a lack of control. This is where statistical sampling may be used to allow a generalist comment based on the results of a predetermined number of transactions. We have already agreed that one can only give an overall opinion on the entire database where the sample has been statistically prepared.

Getting management to act on audit recommendations Ensuring that internal audit recommendations are supported by indicating the extent of risk in failing to take remedial action encourages management to adopt them. So where we find excessive levels of non-compliance with a key control, this must be quantified and set against the corresponding recommendation.

Highlighting implications of failure to act on identified control weaknesses We use statistical sampling to predict the extent of uncontrolled error. This need not be in terms of one-off examples that give no indication of the scale and extent of the problems as in some audit reports. Scientific sampling can result in matrix boxes in the report where the type of errors found can be given global values based on extrapolation, to increase the impact of the findings.

Statistical sampling is a means to an end. It assists in achieving defined test objectives, without examining the entire population. The role of statistical sampling within the testing routine is described in Figure 9.22.

Sampling Techniques

There are two main aspects to statistical sampling. One is how the number of items to be examined is defined. The other relates to the methods used to extract the required information. The latter is called the sampling method or selection technique. Methods used to define numbers tested are called sampling plans. This section deals with sampling methods and these may be set out as:

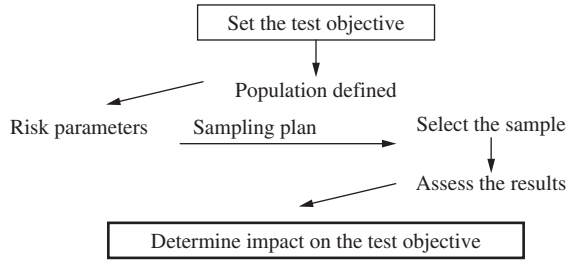


FIGURE 9.22 Testing using statistical sampling.

Random sampling This technique is used to select samples such that each item in the population has an equal chance of being chosen. Random number tables may be used to choose the required items and these may be generated by an appropriately programmed software.

Stratified sampling If we recall that the normal distribution places values in the shape of a bell, then a skewed distribution will not appear symmetrical. This may mean that the auditor can divide the population into several segments that may consist of, say, a small number of high-value invoices for revenue contracts and a large number of small-value ones for one-off supplies. The auditor may wish to pay more attention to high-value items and in so doing can split the population into two and apply statistical sampling plans with different confidence levels to each one. The auditor may have decided that payments to overseas agents are not adequately controlled and there is a significant risk that many such payments may fall foul of anti-corruption legislation and may wish to examine a sample of these payments. The population of payments to 1,755 overseas agents may be divided into strata, as shown in Figure 9.23.

Stratification:

£ Amount	Number	£ Total amount
0 – 9,999.99	1,400	2,800,000
10,000 – 19,999.99	150	2,000,000
20,000 – 29,999.99	65	1,500,000
30,000 – 39,999.99	35	1,200,000
40,000 – 79,999.99	45	2,500,000
80,000 and over	60	20,800,000
	1,755	30,800,000

FIGURE 9.23 Stratified sampling.

The auditor may wish to examine all 60 payments over £80,000 and then extract a sample of 100 further payments using three value-based strata:

Stratum	£ Range	Total amount	Initial sample
1	0–9,999.99	2,800,000	28
2	10,000–29,999.99	3,500,000	35
3	30,000–79,999.99	3,700,000	37
	80,000 and over	20,800,000	
		30,800,000	100

The initial sample of 100 items distributed per value:

$2.8 + 3.5 + 3.7 = 10,$ which gives $2.8/10 \times 100 = 28, 3.5/10 \times 100 = 35, 3.7/10 \times 100 = 37$

and then all 60 that are over £80,000.

Cluster sampling This is a convenient way of selecting items for testing where once the number of transactions has been defined, they are then taken from one filing area. This may be a single drawer of a filing cabinet and is based on simple working practicalities.

Interval sampling Here the population should be homogeneous, with no cyclical bias or missing items. If we divide the population size by the sample size then the sampling interval is obtained and every *n*th item is chosen for testing. One might imagine a computer being asked to select, say, every 20th item from a particular file.

Automated sampling This may be seen as a selection technique where the auditor uses sampling software to set parameters, determine the number for testing, access the relevant file and then download the selected items into a separate spreadsheet for later analytical testing by the auditor.

Setting Risk Parameters

Statistical sampling is based on probability theory and as such one must set upper and lower limits within which the results may be placed. It is similar to saying that on an average a die will fall on the number six on 1/6 occasions. With statistical sampling one has to set the criteria within which the results should be evaluated and this falls under three basic parameters:

Error rate This is the level of error that one may expect from the population being tested. Error may be seen as, for example, the number of invoices that are incorrect. This is normally set at 5% and most statistical sampling tables are based on this figure. If the actual error rate is different then a revision to the quoted risk boundaries has to be made. The rate is determined by the auditor and is based on pilot studies, discussions with management and the results of previous audits.

Confidence This is the degree to which the results derived from the sample will follow the trend in the actual population. A 95% confidence means that 95 out of every 100 items examined will reflect the population. The position on confidence levels is as shown in Table 9.5.

TABLE 9.5 Confidence levels.

Level	*Perception*
Below 90%	Is too low to be of any real value
90%	Is where the auditor knows a lot about the population but wishes to convince management
95%	Is the level that is generally used and is high enough to satisfy the auditor and management
99%	Is too high and will result in most of the population being selected

Precision This shows the margin within which the results can be quoted and defines the degree of accuracy that is required. It may be in terms of the quoted error being expressed as a figure

taken from testing the sample plus or minus the degree of precision, say 2%. The real result relative to the population will be somewhere within the lower and upper levels. If one needs to be accurate to 2% one may find an error in the sample of, say, £100; this may be quoted for the population between £98 and £102. The level chosen will depend on the objective of the test and how the results are used.

Extrapolation This occurs when results taken from a sample are grossed up and applied to the whole population. The average result from the sample is multiplied by the value of the population to give the estimated total error. Risk parameters are set by the auditor and depend on the test objective. It is practice to use 5% error rate tables, with 95% confidence at plus or minus 2% precision. Using these standards, most statistically extrapolated results will be accepted by management.

Audit Testing and Statistical Sampling

The two main types of audit testing are compliance and substantive testing although one may perform some walk-through tests during the ascertainment stage. Note the following:

- **Compliance tests.** Here one is testing the existence or otherwise of a particular control. The test is of a yes/no nature where an attribute (i.e. control adherence) is either present or does not exist. An example may be a test to determine the number of purchase invoices that have not been authorized by a designated officer before being paid.
- **Substantive tests.** These tests are carried out to establish the extent to which the implications of a control weakness may be quantified. We may be concerned to discover the total value of purchase invoices incorrectly posted to the wrong year due to poor cut-off procedures.

These two testing conventions require different statistical sampling plans geared into the objectives of the tests. Compliance testing is concerned with specific attributes so that a frequency may be quoted. Substantive testing looks for variables and enables the auditor to quote a range of values from the test results. The sampling plans as shown in Table 9.6.

TABLE 9.6 The sampling plans.

Compliance testing	*Substantive testing*
Attribute sampling	Variable sampling
Stop–go sampling	Difference estimates
Discovery sampling	Monetary unit sampling

Compliance testing requires variations of attribute sampling, while substantive testing is based on variations of variable sampling. These plans are expanded below.

The various sampling plans Each of these sampling plans will be briefly dealt with. It is important to appreciate where each plan may be applied in determining the number of items to examine. Graham Westwood (from unpublished course notes from a Masters degree programme, City University Business School, 1991) has suggested a criterion for selecting the most appropriate plan:

Quantitative features (substantive tests):

Is the book value of the population available?

If no – use variable sampling.

If yes – do we expect a difference?

If no – use MUS (Monetary unit sampling).

If yes – use difference estimates.

Qualitative features (compliance tests):

Is fraud suspected?

If yes – use discovery sampling.

If no – do we expect a low error rate?

If no – use fixed attribute sampling.

If yes – use stop-go sampling.

Substantive Testing Sampling

Variable sampling This plan enables one to take the average result from the sample and extrapolate this to arrive at an estimated error rate that applies to the entire population. A preliminary sample of 50 items is taken and the error rate calculated along with the SD from the sample. The error rate divided by the SD gives a proportion that can be used to determine sample sizes from the table for various confidence levels. For additional items the SD is recalculated.

Difference estimates Where the book value (BV) is available one may take the difference between the BV and actuals for a preliminary sample of 100 items. The resulting SD is used to calculate the new sampling error rate that may be compared to the original. This technique provides a short cut and can be very convenient. If there are many missing items then the differences may actually be bigger than the BV.

Monetary unit sampling (MUS) This plan is used by external auditors and incorporates an assessment of the strength of the particular internal control system. The poorer the internal controls the greater the degree of reliability required, which in turn makes the sample size larger. One assumes that the population consists of a series of values and in so doing the larger (and more material) items are naturally selected once the sampling interval is determined. One is looking for an over- or understatement of monetary values so that the auditor can decide whether the account may be accepted or not in an audit opinion. Accordingly one is able to sample, say, the debtor's figure and examine all the larger items before deciding if the balance sheet figure is correctly stated (i.e. not overstated). An MUS plan may give the result that out of a population size of £100,000, 60 items should be examined which are selected at intervals of £1,667.

There are **advantages** of this plan:

1. One only needs the value of the population and not the actual number or the SD.
2. The confidence level is determined by the reliability of the system of internal control.
3. High-value items are always included in the sample.

There are also several **disadvantages**:

1. It is biased towards high-value items that may in fact be better controlled than lower value ones.
2. No error can be defined for the population.
3. It will ignore nil-value items.
4. It is used only for accept/reject decisions.
5. One needs to know the total value of the population.
6. A low confidence level will dilute the results.
7. It is a complicated technique to apply in practice.

Compliance Test Sampling

Attribute sampling One needs to set an error rate, confidence levels and precision limits. This may be a 5% error at 95% confidence plus or minus 2%. The error rate determines which statistical sampling table is used and this table will give the required sample size at a glance. When one determines the actual error rate then the precision is recalculated for errors over the set rate. Additional error rate tables are used with the new error rate for the revised precision levels.

Stop-go sampling This is an incremental sampling plan that starts with smaller samples to save time once one sets an acceptable probability level. The plan assumes that all populations over 2,000 are the same. The sample will give a maximum acceptable error rate of, say, 5% and if the actual results are higher, then further samples are taken until the results are acceptable and within the set limit.

Discovery sampling Discovery sampling is based on the notion of determining how many items must be examined if one has a fair chance of discovering a suspected fraud. The plan gives the sample size required to find the error and is useful for planning purposes, although no conclusions may be drawn about the population itself. As with all sampling plans one must set a probability within which fall the chances of discovering the fraud with the sample size that the table provides.

Some Basic Rules for Applying Statistical Sampling

Some auditors never use statistical sampling while others have a policy of applying this technique whenever possible. External auditors are more prone to rely on mathematically based samples in deciding whether or not a financial statement is acceptable. While internal audit theory makes it clear that the use of statistical sampling is by no means mandatory, there are rules originally developed by Graham Westwood that should be applied when deciding when it might be appropriate:

1. **Only use statistical sampling where it is appropriate.** The auditor makes a conscious decision at this stage rather than an instinctive view that it is not normally used. The audit unit should set out clear rules on the application of statistical sampling and these should be fully documented in the audit manual. Not only will this act as a source of guidance, but it will also provide a mechanism by which audit management needs explanation where the technique was not used when the audit manual indicates that it should be. By the same token, the rules should stop the auditor from exploring the statistical process where it is inappropriate, say, for smaller fields or where the population is unknown.

2. **Define and know the population.** Where the technique is applied there needs to be a formal process whereby the item that is being considered is fully researched by the auditor. This process will bring the audit to a higher level as this research will highlight what the auditor is reviewing, which in itself brings many benefits. It may well be that the act of getting to know the population (say a specific database) will bring findings relating to the quality of the information itself. If in a debtors system we could not extract the total value of debt at any one period, we may feel that the report generator may not have been properly established. Furthermore, management does not have access to high-level information fundamental to the control of the debtors system.
3. **Ensure that every item has an equal chance of selection.** Randomness is the main ingredient of statistical sampling as this supports the objective way that the technique should be applied. It is satisfying to be able to justify a sample that is selected through the principle of random selection. This can become an issue where the sample contains sensitive items that management may feel are being targeted by the auditor. Audits of payroll or personnel systems can experience this problem. It may be that the auditor is accused of missing out senior figures in the organization or, say, victimizing named persons who have had some conflict with the audit service in the past. The random selection process defeats all these concerns as items are selected and examined with no in-built bias.
4. **Ensure that patterns do not affect the randomness.** The population should be capable of supporting random sampling in the way it is formed and maintained. Statistical sampling cannot fit all circumstances and this point should be fully recognized if it is to have any use at all. There are certain investigations relating to fraud, irregularity and breach of procedure where the auditor is looking for particular items and has to be very selective in the way the available information is analysed. Where the auditor wishes to inject his/her own supposition into the appraisal of data, this militates against the random methods that underpin statistical sampling.
5. **Where judgement sampling is used one may not form definite conclusions about the population.** The rules on the application of extrapolation mean, even where management is not aware of this, rough figures cannot be projected without a scientific base. Any such predictions should be qualified along the lines such as 'a rough estimate of the effect of these errors on the entire system, although not statistically valid, would fall at a level of some £xyz'. A formal projection would have to have a scientific base where the auditor would be able to state for example 'there is a high probability that the extent of total error falls within the ranges £z to £y'.
6. **Use an error rate that is reasonable.** The error rate is built into the statistical tables and is based on assumptions about the population. The required rate is based on the auditor's knowledge about this population and this should be assessed carefully.
7. **Stratify the population where this reduces variability.** We have touched upon the position where the auditor wishes to follow a certain line of enquiry, and is hindered by the need to assume a neutral stance by the use of statistical sampling. Stratification allows the auditor to profile the population in a way that suits the audit objective. If, for example, we are concerned about high-value items in a certain system then we can divide the database and treat them to special attention by assigning a tight set of risk parameters that mean most of them are examined. The other transactions may be given less severe treatment (through the use of lower risk parameters). We can go on to suggest that low value (or low significance) matters may be more or less ignored through the further use of stratification.
8. **Do not set needlessly high reliability goals.** There are accepted standards that reflect the general business environment. The use of 95% confidence, plus or minus 2% precision

with a 5% error rate, is normally sufficient to draw reasoned conclusions about the system under review and this may be used as a good starting place. The audit manual should provide suitable direction on this matter.

9. **Analyse the results carefully.** Statistical sampling is a means to an end and results must make sense and fit the audit objective. What comes out of the testing routines must make sense. One way of ensuring this happens is to keep in mind the report format when applying any technique to promote basic questions relating to the way the resultant material contributes to the final audit opinion.

Testing secures material to support the audit findings and that can be of use when formulating the audit report. The results are used to confirm or not the auditor's opinion in a way that can be communicated to management. Compliance tests can be quite straightforward as long as one understands the control that is being tested. Substantive tests may pose problems. The auditor may set up as an expert in determining whether something has been successful. Care is required and the auditor should remember the overriding objective of securing adequate management action to solve real and material control weaknesses that affect the success of the operation/organization. Working papers hold the documentation that results from the testing process which is why it is included here. The audit manual should establish standards for documenting audit work and retaining necessary information. There should be defined disposal dates for what will eventually be confidential waste. It is essential that these standards are high and contribute to the overall efficiency of the audit process. Moreover, the CAE should establish suitable reviewing mechanisms to ensure that these standards are being properly adhered to throughout the audit department. Janet L. Colbert has provided some advice on the use of audit sampling:

> Before becoming enmeshed in performing sampling procedures, internal auditors should step back and first consider whether this technique is appropriately suited to the task at hand. In certain circumstances, sampling is simply not the best approach; and depending on other information gathered for a particular area, performing a sample may not be necessary. Sampling also affects the reliability of results; whereas an examination of 100 percent of a population produces results with high reliability, sampling decreases reliability. In addition, auditors produce different types and amounts of workpaper documentation depending on whether sampling, or another approach, is utilised. As with any examination procedure, sampling should be used judiciously, as a poor decision can lead to inaccurate results. Auditors need to make sure that the target population meets the necessary criteria for conducting a sample before applying this technique. When used appropriately, sampling can add significant value to the audit process by increasing efficiency and effectiveness of testing procedures.[10]

Statistical sampling is not a mandatory technique although it should not be ignored by the auditor as it can be used to comment on a system through the use of a relatively small sample. The audit department should define a clear policy on the use of this technique and where and how it should be applied, and this should appear in the audit manual. The use of automated statistical sampling via a suitable software package assists getting auditors to use statistical sampling. If judgement sampling is, in the main, being applied this should be stated as clear policy having reviewed the applicability of statistical sampling.

9.8 Reporting Results of the Audit

Some auditors argue that the audit report is the fundamental end product of any audit and IIA Performance Standard 2400 states that: 'Internal auditors must communicate the engagement

results.' In reality the impact of the audit should be the actual changes that are created as a result of the investment of audit resources and here the report forms just part of this process. Whatever the view, the fact is that audit reporting is one of those fundamental techniques that must be mastered by the auditor. Sawyer has made clear that: 'Reports are the auditor's opportunity to get management's undivided attention. That is how auditors should regard reporting – as an opportunity, not dreary drudgery – a perfect occasion to show management how.'[11]

There are many components and principles that underlie audit reporting, the most important of which is the quality of audit work that has been carried out prior to the reporting stage. Reporting is important and a useful phrase to express this importance comes from the IIA Handbook Series: 'an auditor's greatest idea or discovery is only as effective as his or her ability to express the concept to others and elicit the desired response'.[12]

Types of Reports

Auditors are involved in many different types of report:

1. Annual audit reports This annual report to the organization may be presented to the audit committee and will have two main components. It should set out and discuss the audit achievements according to the annual plan. In addition, it should provide a summary of key areas tackled and any material issues concerning the adequacy of the organization's system of risk management. In this respect, it acts not only as a control over the performance of internal audit, but also as a major control over the entire organization. This latter attribute means that major control issues that have not been adequately addressed will be isolated and brought to the attention of senior management of the organization. Accordingly, this should be used with great care since it represents the ultimate fail-safe mechanism where all other efforts to get the audit message across have failed. In addition to the general areas that will be discussed, there might be specific failings that will be highlighted for action.

2. Quarterly audit reports This is a more detailed version of the annual report and one would expect that most matters in the quarterly plan will have been dealt with. Accompanying statistics on chargeable hours and productivity should also be published and it is good practice to indicate how much each completed audit costs in terms of hours charged (times hourly rate). This is more a control over the audit function than a reflective statement on organizational controls that is a feature of the annual report. Again quarterly reports should be linked to the underlying plans. The current economic environment makes it much more difficult to plan and as such the quarterly period has greater significance than the annual one. An efficient auditor time monitoring system should provide information that can be incorporated directly into the quarterly report.

3. Monthly progress reports Some chief internal auditors require a monthly progress report setting out the status of each main audit and this may be followed up by progress meetings to deal with potential delays and inefficiencies. This can be an important control that enables the CAE to keep tabs on audit work paying particular attention to aborted audits or those that appear to be in progress for an unduly long period. Suspended work creates additional problems and it is not advisable to have projects that are dealt with on a continuing stop-start basis. It is more difficult to find excuses on a monthly basis in contrast to the quarterly report where inefficiencies may be hidden by excessive details of completed audits. This monthly snapshot can expose problems and has a further advantage in that it can greatly assist resource rescheduling where required. Armed

with a monthly account of progress, the CAE may take comfort in the way that audit managers are deploying their resources.

4. Preliminary survey reports Before formal terms of reference can be formulated and planned hours defined, we have to do a fair amount of background work. This is called a preliminary survey and the work should result in a preliminary survey report (PSR). Appendices to this report should include a draft assignment plan, audit approach and audit objectives. The PSR itself should be concise and normally not more than two pages long. This will allow the audit manager to formulate an assignment plan. While the report itself cannot contain findings in terms of evidence of control weaknesses, it may outline 'suppositions' which may be described as potential control weaknesses.

Interim Audit Reports

Before the full audit report is produced one would expect interim reports particularly on larger projects. These have three main uses:

1. It forces the auditor to build the report as work progresses. As such the findings are fresh in the auditor's mind as they appear and are captured in written format. This allows a greater link between the audit report and underlying work that is being carried out by the auditor. Furthermore, it should be possible to complete a draft audit report quite soon after the field work is finished and not have to wait unduly long periods for the report to be made available.
2. It keeps the audit manager up to date and allows interim reviews of work performed. If the audit has to be aborted or suspended for any reason, then it is possible to report the results to date very quickly. This will act as a position statement that may be picked up again when the audit is being resumed. The worst case scenario occurs where the auditor introduces the audit to managers and heightens their expectations, carries out detailed audit work and after several weeks appears to disappear completely. Just when the managers have forgotten the audit, a draft report appears on their desk that contains many surprises. The correct model is where the auditor briefs management at the end of each week on findings to date and general progress on the audit. This is where the interim report comes to the auditor's aid as a useful communication device.
3. In this way it may be given to the client and so act as a continuous report clearance device as well as bringing the client into the audit process itself. Furthermore, it is possible to produce the final draft shortly after conclusion of the field work. This approach will also allow audit to comply with the IIA reporting standards which suggest that nothing in the report should come as a surprise to management. In fact the IIA IPPF Performance Standards endorse this view and says that:

   2410 – Criteria for Communicating: Communications must include the engagement's objectives and scope as well as applicable conclusions, recommendations, and action plans.

   2410.A1 – Final communication of engagement results must, where appropriate, contain internal auditors' overall opinion and/or conclusions.

   2410.A2 – Internal auditors are encouraged to acknowledge satisfactory performance in engagement communications.

   2410.A3 – When releasing engagement results to parties outside the organization, the communication must include limitations on distribution and use of the results.

   2410.C1 – Communication of the progress and results of consulting engagements will vary in form and content depending upon the nature of the engagement and the needs of the client.

Audit Assignment Reports

This is what most auditors think of when considering the topic of audit reports and it is dealt with in some detail below:

1. Executive summaries A two or three page summary can be attached to the front of the report or issued as a separate document. It provides a concise account of objectives, main conclusions and the steps that management should be taking. This recognizes that managers are busy and wish to take a short cut in getting to grips with any material issues that may result from an audit. A groundbreaking article that helped focus audit effort to top executives was produced in 1997 by Francis X. Bossle and Alfred R. Michenzi on the One Page Audit Report:

> Previously, our misguided audit goal was to create an all-inclusive final document that would make sense to all users, from the operating level all the way up to the CEO. We constructed long narratives that gave everyone a detailed analysis of the audit findings. As a result, completing and distributing the final report usually required several months. Unfortunately, the report was often dated and of limited usefulness by the time it was eventually issued . . . Our solution to this dilemma was to develop a series of one page audit reports.
>
> 1. ***One Page Audit Report*** – supplies executive management with a nuts and bolts summary of the audit findings and recommendations and covers – subject, responsible officer, scope, risk exposure, overall audit comment, significant audit recs, management response, planned follow up.
> 2. ***Corrective Action Report*** – addresses each audit finding and concerns and covers – title, observation, risk, recommendation, implementation date, management response, department responsible.
> 3. ***Special Project Report*** – addresses limited scope activities of internal audit, covering – subject, nature of request, procedures informed, key audit concerns, contribution of internal audit, follow up action.
>
> Operating management reviews and comments on all three reports, but only the One Page Audit Report and the Special Project Report go to executive management . . . Our one page reporting process has become a win-win situation for everyone involved. Overall customer satisfaction with the efforts and work of our department has improved.[13]

2. Follow-up reports All audit work should be followed up and it is possible to establish a standardized reporting format to check on outstanding audit recommendations. These audits tend to be simple to perform but sensitive in nature. They involve forming a view on whether management has done all that it promised to. Practice Advisory 2500.A1-1 deals with the follow-up process:

> 2500.A1 – The CAE must establish a follow-up process to monitor and ensure that management actions have been effectively implemented or that senior management has accepted the risk of not taking action.
>
> 1. Internal auditors determine whether management has taken action or implemented the recommendation. The internal auditor determines whether the desired results were achieved or if senior management or the board has assumed the risk of not taking action or implementing the recommendation.
> 2. Follow-up is a process by which internal auditors evaluate the adequacy, effectiveness and timeliness of actions taken by management on reported observations and recommendations,

including those made by external auditors and others. This process also includes determining whether senior management and/or the board have assumed the risk of not taking corrective action on reported observations.

3. The internal audit activity's charter should define the responsibility for follow-up. The CAE determines the nature, timing and extent of follow-up, considering the following factors:
   - significance of the reported observation or recommendation;
   - degree of effort and cost needed to correct the reported condition;
   - impact that may result should the corrective action fail;
   - complexity of the corrective action;
   - time period involved.

1. The CAE is responsible for scheduling follow-up activities as part of developing engagement work schedules. Scheduling of follow-up is based on the risk and exposure involved, as well as the degree of difficulty and the significance of timing in implementing corrective action.
2. Where the CAE judges that management's oral or written response indicates that action taken is sufficient when weighed against the relative importance of the observation or recommendation, internal auditors may follow up as part of the next engagement.
3. Internal auditors ascertain whether actions taken on observations and recommendations remedy the underlying conditions. Follow-up activities should be appropriately documented.

It may be necessary to criticize management where it has failed to implement agreed recommendations while at the same time maintaining a degree of diplomacy. It is necessary to weigh up all excuses for a lack of action before deciding whether management has acted reasonably. The follow-up process is crucial and IIA Performance Standard 2500 states that: The chief audit executive must establish and maintain a system to monitor the disposition of results communicated to management. Assurance and consulting work is covered in the following IIA standards:

2500.A1 – The chief audit executive must establish a follow-up process to monitor and ensure that management actions have been effectively implemented or that senior management has accepted the risk of not taking action.

2500.C1 – The internal audit activity must monitor the disposition of results of consulting engagements to the extent agreed upon with the client.

Follow-up procedures revolve around the view of residual risk. Where the internal auditor has failed to convince client management that the risk needs addressing then any associated audit recommendations may not be agreed upon. Where the internal auditor is convinced that this level of residual risk is outside the remit of the corporate risk appetite then the matter should be reported upwards, even up to the board. Performance Standard 2600 deals with this tricky issue and says:

When the chief audit executive believes that senior management has accepted a level of residual risk that may be unacceptable to the organization, the chief audit executive must discuss the matter with senior management. If the decision regarding residual risk is not resolved, the chief audit executive must report the matter to the board for resolution.

Performance standard 2410 covers communicating audit work:

Communications must include the engagement's objectives and scope as well as applicable conclusions, recommendations, and action plans.

There are other standards that provide more detailed requirements depending on the type of audit in question:

2410.A1 – Final communication of engagement results must, where appropriate, contain internal auditors' overall opinion and/or conclusions.

2410.A2 – Internal auditors are encouraged to acknowledge satisfactory performance in engagement communications.

2410.A3 – When releasing engagement results to parties outside the organization, the communication must include limitations on distribution and use of the results.

2410.C1 – Communication of the progress and results of consulting engagements will vary in form and content depending upon the nature of the engagement and the needs of the client.

3. Fraud investigation reports These reports detail the allegations, the work carried out and why, as well as the main findings. It is extremely frustrating to pick up a file on a fraud investigation and see no concluding audit report covering the case. This is a mistake that many auditors make and the audit standard that requires us to report the results of audits applies equally to all types of work.

4. Oral reports Auditors are charged with reporting the results of audit work and this may be in an oral format. Oral reports are designed to save time and can have a more direct impact on the recipient. They also allow the audit client to provide instant feedback to the lead auditor.

Staff Appraisal Reports

All auditors should have on file appraisal reports and these should flow from the performance appraisal scheme. It is generally advisable to link these reviews into individual development programmes. The audit manager will draft this report after discussions with the auditor in question.

The Reporting Process

Audit reports are not simply published documents but are the result of a comprehensive audit reporting process that may be summarized in Figure 9.24.

We discuss the components shown in Figure 9.24:

Preliminary survey and assignment plan The audit report actually starts with a plan that sets the framework for the ensuing audit.

Clear audit objectives The next key stage in the reporting process appears in the form of an overall goal. This gives direction for the work and ensures that the report is based around an agreed objective, which will be stated in the report itself. The IIA Performance Standard 2410 requires that: 'Communications must include the engagement's objectives and scope as well as applicable conclusions, recommendations, and action plans.'

Good audit work There is very little that can be gained from an audit without ensuring that the underlying work it is based on has been performed to acceptable standards. The downfall of

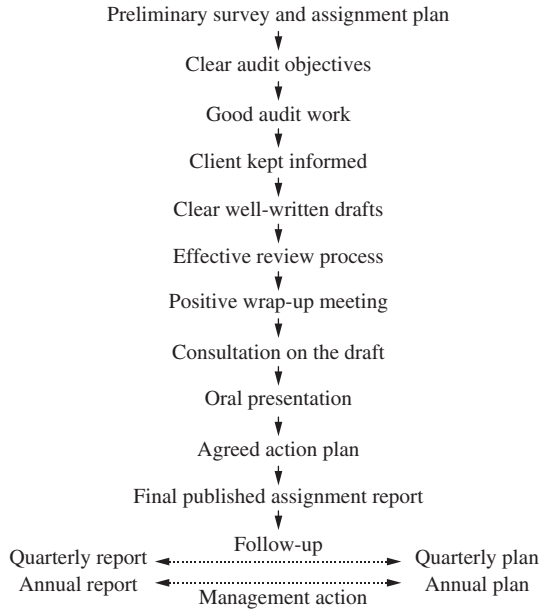


FIGURE 9.24 Audit reporting process.

many a report is to emphasize a flowing and attractive terminology and reporting style without having done sufficient basic hard audit work. There are no short cuts to this as fabricated material couched in indecisive terms will eventually be unmasked for exactly what it is. This position occurs where reports are based around gossip, rumour and hearsay in contrast to professional audit work. This is why the review process should include a consideration of working papers and not just the report that the auditor presents to the audit manager.

Client kept involved Keeping the client up to date and involved in the audit process leads to a better report. Some auditors feel that findings should be withheld from the auditee until the report is made available, for fear of action taken now by management 'spoiling' the impact of the report. This is a distorted view of the audit role which is not to claim victories (i.e. findings) at management's expense. In reality it is to help and assist management in the discharge of its responsibilities. Any findings should be brought to the attention of management in regular progress meetings. These findings may nonetheless be quoted in the report, and the fact that management has already acted on them strengthens rather than weakens the impact of the audit.

Clear well-written drafts The way a report is written does affect the way the findings, conclusions and recommendations are received. Good audit work, based around close contact with the auditee provides a foundation for a well-received report, but the actual words presented form a defined vehicle for communicating the findings. In this sense the report must be based on professional standards of presentation that lift the audit in the eyes of the reader. Meanwhile the auditor will provide a view of the adequacy of risk management and internal control in line with Performance Standard 2410.A1 which states that: 'The final communication of results should, where appropriate, contain the internal auditor's overall opinion.' Well-written reports use plain English and the official Plain *English Writing Guide* explains:

> What's plain English – It is a way of writing that gets your meaning across clearly, concisely and with the effect you want, to your intended reader. But it is not enough to be clear and concise. Always consider your reader's feelings. This means putting yourself in your reader's shoes and asking yourself 'how would I feel if I received this message'. If you think of plain English writing as being:
>
> - clear
> - concise
> - human
>
> you won't go far wrong.[14]

One way of ensuring clear reports is to establish a reporting guide and give examples of words that are jargonized and those that are much preferred, for example:

Jargon	**Preferred**
due to the fact that	because
endeavour	try
evaluate	test, think about
expeditiously	promptly
facilitate	help, ease
finalize	finish
for a period of	for
for the reason that	because
generate	produce
have been shown to be	are
implement	do, carry out

Effective review process The two key points to the review stage of the reporting process are that first, this review should ensure that the report is prepared to professional standards that fit with the underlying work that has been completed. Second, it should be completed without delaying the swift progress of the draft report. If these two principles are firmly in place, despite the fact that they conflict with each other to an extent, then the report process will tend to be successful. The audit manager should review the report using a predetermined criterion, along the lines suggested by the IIA Performance Standard 2420 which dictates that: 'Communications must be accurate, objective, clear, concise, constructive, complete and timely.'

Positive wrap-up meeting It must be said that one of the most stressful parts of an audit is the face-to-face closure meeting that is held once the field work has been completed. Much will depend on the relationship with the client that has been built up during the audit and the extent to which findings have been discussed as they arise. Whatever the scenario, we would hope that the auditor does not seek to avoid this stage, as it is an important component of successful reporting.

Consultation on the draft We would next wish to see a formal process whereby the draft report is sent to all parties affected by the recommendations. This is based on best practice and standards that ensure fair representation for all individuals that have a role to play in acting on audit findings. The report should have balance and IIA Performance Standard 2410.A1 declares that:

> 'Final communication of engagement results must, where appropriate, contain internal auditors' overall opinion and/or conclusions.'

Oral presentations It is as well to stage an oral presentation for audits that are more complicated and/or address sensitive matters. This provides an opportunity for feedback and promotes a process whereby the auditor justifies the assumed position. Both these factors have to be satisfied if we are to get effective action based around audit recommendations.

Agreed action plans We arrive at the negotiation/agreement stage that is also part of the reporting process. This will enable us to present management's proposals within the report so as to make it an active working document that has meaning to both audit and management. Where the internal auditor needs to enter into the realms of pure negotiation in trying to drive home, say, the significance of specific risks to information security that are not being properly addressed, then support is available from a book, *The New Negotiating Edge, the Behavioural Approach for Results and Relationships*, which highlights three styles of negotiating:

- Red style – tough, aggressive, manipulative – taking behaviour
- Blue – softer, kinder and win-win based – giving behaviour
- Purple – balance, consistent set of behaviours, resolute determination to resolve differences based on merits of the case and trade agreements.

The authors see negotiation as getting what you want from somebody by exchanging with them some of what they want. They go on to describe four phases in the negotiations that can be used to ensure a smooth transition between the phases:

- Prepare – What do we want? Can we out prepare the other part?
- Debate – What do they want? Communication is essential here.
- Propose – What wants could we trade? Tentative solutions. Nothing really happens until we start proposing. Purple = if-then words recognizing both sides.
- Bargain – what wants will we trade? Specific to what they want.[15]

Final published assignment report A final report should be prepared along with a clear definition of reporting lines and people who should be given copies. There are many audit units guilty of producing 'draft' reports that remain in circulation without a final version, much to the confusion of all involved with this document. Where there are problems with the accuracy of the final report these should be corrected. The IIA Performance Standard 2421 sets a direction here: *'If a final communication contains a significant error or omission, the chief audit executive must communicate corrected information to all parties who received the original communication.'*

It may also be an idea to consider any developments that have occurred since the completion of the audit field work and refer to them in the final report if appropriate. Meanwhile, two draft IIA standards address the publication of audit reports to external parties:

2201.A1 – When planning an engagement for parties outside the organization, internal auditors must establish a written understanding with them about objectives, scope, respective responsibilities, and other expectations, including restrictions on distribution of the results of the engagement and access to engagement records.

2201.C1 – Internal auditors must establish an understanding with consulting engagement clients about objectives, scope, respective responsibilities, and other client expectations. For significant engagements, this understanding must be documented.

Follow-up The process is still not complete until we have set up a follow-up routine in line with best audit practice. These standards can be mentioned within the report or the accompanying letter.

Quarterly reports The audit report should feed into the quarterly reporting cycle that seeks to summarize what has been found and reported on in the relevant three-month period. Reference to the quarterly plan makes this a dynamic process that is linked to a defined reference point.

Annual report The above is equally true for the annual reporting cycle that again should be set within the context of the plan for the year in question.

Management action We arrive at the true audit product in terms of management action based on the audit report. All else is simply to set a foundation within which this action may be stimulated by the auditor. The objective of the reporting process is to get management to act on audit's advice. A report that suggests no action is required is just as significant as one that asks for many changes. Assurances (of good control) allow management to channel resources into riskier areas. The reality of corporate life is that there are many reports and other types of communications that bombard managers. This problem has been highlighted by many writers:

> The average Briton is bombarded with more that 4,000 messages every day – from e-mails to mundane washing instructions on clothes – says a report. Just travelling to work can expose people to 150 messages, including adverts and newspaper headlines, according to the research. And a trip to the supermarket is likely to mean reading up to 1,600 different messages, beginning with car parking instructions outside the store and then being faced with a multitude of information on the goods inside. As a result, Britons are suffering information overload, the report concludes. But it seems that as the problem has grown, people have become adept at screening all the messages and ignoring the vast majority that do not affect them.[16]

It is essential that the entire reporting process is carefully managed and controlled since a failing in any one component will impair the impact of the report. Note that the final result of this process may be defined as 'management action' to secure changes and improvements to the way the organization designs, implements, seeks compliance with and reviews its systems of internal control. There are auditors who complain that managers fail to implement audit recommendations and that they should be disciplined accordingly. In practice, however, most of the blame can be placed on a failure by audit management to implement a suitable reporting process based on the concepts set out above. An apt comment from the late Joe Morris made in 1997 is still relevant today: 'An internal audit report that talks about yesterday is no good at all.'[17]

Performance Standards

'2440.A1 – The CAE is responsible for communicating the final results to individuals who can ensure that the results are given due consideration.' Much may be said about defining the client for audit services and this may vary according to the situation and arrangements made. The client concept has to be treated with flexibility. The guiding principle that should be applied to audit reports is that they should be addressed to the party who would be most effective in making the necessary changes required. In fact, the IIA Performance Standards requires that:

2440 – Disseminating Results: The chief audit executive must communicate results to the appropriate parties.

Interpretation: The chief audit executive or designee reviews and approves the final engagement communication before issuance and decides to whom and how it will be disseminated.

2440.A1 – The chief audit executive is responsible for communicating the final results to parties who can ensure that the results are given due consideration.

2440.A2 – If not otherwise mandated by legal, statutory, or regulatory requirements, prior to releasing results to parties outside the organization the chief audit executive must:

- Assess the potential risk to the organization;
- Consult with senior management and/or legal counsel as appropriate; and
- Control dissemination by restricting the use of the results.

2440.C1 – The chief audit executive is responsible for communicating the final results of consulting engagements to clients.

2440.C2 – During consulting engagements, governance, risk management, and control issues may be identified. Whenever these issues are significant to the organization, they must be communicated to senior management and the board.

'The CAE is responsible for communicating the final results to individuals who can ensure that the results are given due consideration.' This will depend on the type of organization, the type of audit work performed and the circumstances of the audit. Ordinarily the report will go to the line manager for the area under review and the next tier up.

Objectives of the Audit Report

Extensive audit resources may be spent on performing an audit and the client may see as the end product a published audit report. It is therefore important that the objectives of this final document are clearly established and this may be one or more of the following:

1. To recommend change The audit report must be first and foremost about securing change in terms of new or improved controls. The technique of describing the current control failings should be used to help stimulate change by bringing home the problems that must be overcome. This concept can become somewhat blurred where the auditor/client relationship develops to a state of 'one-up-manship'. To criticize, to find fault, to expose and to search for the implications of poor risk management are subsidiary matters compared to the main point of getting something done about these problems. In short, the audit report should primarily be aimed at this idea of change, with the recommendations being the single most important component of the document.

2. To provide an insight for management into risk and control issues It can be said that the audit report will highlight the importance of control issues and relate these to risks to management's own business objectives. This places the need for control on the agenda. This is particularly relevant where there is a great deal of change in business operations due to environmental factors and where new systems and procedures are being developed. The audit report may help balance management's goals in driving through major new initiatives, by warning of the potential for danger where the control implications have not been properly addressed. Control requires resources which in turn must be prioritized by management. It is only by placing the need for control on an equal footing with other competing issues that adequate solutions will be provided and here the audit report can have a major role.

3. To secure action in response to audit advice Action goes further than recommendation by moving an idea to the status of an actual event. This turns audit suggestion into real action by allowing management to claim the required changes as its own. This is the main goal of the audit report where one is able to report a management action plan agreed with the parties responsible for making it happen. One broad measure of internal audit performance is how much real action has resulted from audit reports.

> Internal audit reviewed cashiering and the senior auditor had begun preliminary work. In the staff canteen, the chief cashier had an informal conversation with the audit manager responsible for the audit. He said he was urgently writing procedures to deal with cashiering operations so that he would not be 'caught out' by the audit. The audit manager commended this, and said audit would be happy to contribute to developing sound procedures, which surprised the cashier.

4. To bring problems to management's attention Another view of the audit report suggests that it is designed to ensure that management is aware of unmitigated risk and its effect on systems objectives. These reports will feature the results of compliance and substantive testing, setting out the frequency of breaches and level of error. It may be possible to extrapolate these sample results to give an overall conclusion on the population. Client expectation will demand that error, irregularity and other problems are brought out in the report despite being based on misunderstanding of the audit role. It is only the brave auditor who will ignore these expectations when drafting an audit report. Some argue that a true management action plan is based on audit isolating the problem while management provides the most suitable solution.

5. To ensure that the results of audit work are clearly documented Not all audit reports are published and some, particularly preliminary survey reports, are used as internal documents. Others contain no major findings but are still sent out to management. The report represents a formal record of work carried out and the results. It may be necessary to document findings when carrying out a fraud investigation even though these reports may not be sent outside the audit department. The main purpose of these reports is to document the audit. Where management decides not to take up audit recommendations, then the auditor can point to the audit report as the formal device for conveying the audit opinion. This may be useful in the event of a dispute later. This appears at first sight a defensive approach but it is sound practice to use the report as a formal record of the audit.

6. To provide assurance to management on their activities This part of the role of the audit report is based on the view that audit reviews controls, because they may have fallen into disrepair or misuse. There is a preventive approach that relies on the existence of sound controls in the first place. The audit may adopt the guise of providing comfort to management that risk management and controls are sound and are being applied in practice and as such many reports will have no major adverse findings. The lack of control problems should not be seen as a criticism of audit effectiveness or a failure to secure 'Brownie points' in terms of the number of errors/problems found. This would point more to the success of audit in getting the control message across to management who has then resourced the need for good systems. The audit report in this instance will be designed to support management in its drive for better controls. We have argued that assurances that risk management is sound do, in themselves, promote effective management decisions. This is because resources may then be rightly directed towards other areas of higher risk in line with the knowledge provided by the auditor's report.

7. To show managers how their problems may be solved Pointing the way forward is another objective of the audit report. There are many cases where managers are clear as to the nature of problems and sometimes the underlying causes. Their concerns are centred on securing help in solving these problems and it is here that the consultancy role of internal audit comes in. Reports steeped in isolating the implications of residual risk will have little use in this scenario. The application of creative thinking applied to underlying barriers to value for money are the real products the client will be looking for.

8. To provide information about risk management practices This is a valid objective as many audits will report new information that has been specially developed via the audit process. This may be needed to feed into a much wider management decision-making mechanism that may be considering a whole range of options. An example may be performance indicators that have been put together perhaps by a special analysis carried out by the auditors over a range of comparable operational units. This information may be used for many different purposes over a period of time, on the basis that it has been produced by an independent third party (i.e. the auditor) via professional audit techniques. In this case, presentational matters will be important where schedules, tables and graphs would tend to be supplied within the report. For example, a list of large numbers of cheques drawn on the organization that have been returned by the postal service because they could not be delivered. This may highlight a problem with the state of the creditors database (i.e. the address field) and so help direct management attention to this problem.

9. To protect the auditor Many reports will have the subsidiary objective of documenting where audit resources were applied and where it was not possible to do detailed work. This indicates to the client that areas/issues have not been covered with an explanation. It may be used to protect the auditor against later accusations that certain matters were overlooked, which led to defined losses or exposure to high levels of risk. The audit terms of reference and clear qualifications set out within the report will clarify the extent of audit coverage. There is a variety of views and approaches adopted by audit report writers and each has justification. The audit role may be derived from these three objectives. The underlying goal may be to act as a catalyst for all material improvements to controls necessary to ensure that systems objectives are achieved. The four main functions of the audit report are:

- to **assure** management that business risks are well controlled;
- to **alert** them to areas where this is not the case and there are defined risk exposures;
- to **advise** them on steps necessary to improve risk management strategies;
- to support **action** plans prepared by client management.

The internal audit report should reflect the new agenda of corporate governance, risk management and control. Jeffrey Ridley has provided advice on this matter:

> This year watch your language. Create your own dictionary of words and phrases, based on today's internal auditing agenda of 'assurance', 'consultancy' and 'training'. One linked to the IIAInc.'s Glossary and the new image of internal auditing. One that all will understand. Use this to link all internal auditing processes, from charter, recruitment and training to planning, risk assessment, audit programmes and reporting. Use it to influence all those to whom you report and with whom you co-ordinate, including your audit committee, external auditing and other auditors. Use it to create the vision for your services and to market internal auditing professionalism for 2001 and beyond.[18]

Underlying Components of Action

The audit report is the result of a comprehensive process and is a means to an end. There are several clear parts of the audit process that directly impact on the audit report: this working paper is called an internal control evaluation schedule (ICES) and contains details of each major control weakness that appears as an audit finding in the published report. The ICES should contain:

The operational objective This is the business objective, that is, that which the manager is required to achieve. It is essential that this concept is paramount in the search for suitable controls as it sets a frame within which all ensuing work can be contained.

The operational standard This provides the control model against which the current arrangements may be measured bearing in mind the fact that audit is about comparing what is with what should be. This may be seen as the appropriate control mechanism that we would expect to see in place in order to discharge the requirements of the aforementioned operational objective.

The risks of the current practice This constitutes the supposition that is being tested. By comparing existing controls to required controls, one may establish the type of dangers that should be guarded against and so assess the degree of risk derived from the current controls. Risks are expressed in terms of potential problems that should be quantified at some stage in the report.

The deficiency in controls This is a concise statement of what is lacking. It is expressed in terms of control weaknesses and it is these weaknesses that the audit report will seek to remedy by drawing them to the attention of management. The audit report should feature an opinion that summarizes the deficiency in control systems.

The cause of the deficiency Underlying causes must be clearly identified if any progress is to be made in rectifying problems. This is a moot point since it means that the auditor must probe the control weakness to discover why a fault or deficiency actually exists. Where a number of weaknesses can be related to a common fault we are getting closer to a position whereby these failings may be resolved. One such common cause may be a lack of concern by management for formal security arrangements and documentation, which lowers the effectiveness of overall controls. Another may be a view that senior managers are able to override procedures by virtue of their position in the organization, again to the detriment of good risk management and control.

The effect of the deficiency Substantive testing is about defining the effect of control weaknesses. This information will bring home the importance of securing better control and allow management to undertake a form of cost/benefit analysis before committing resources. This will feature as examples of how things can go wrong due to the lack of control and also an overall position, setting out the percentage of breach of procedure and/or error that was found during the audit. These findings should be arranged so they may feed into the draft audit report.

Conclusions An overall audit opinion forces the auditor to consider the wider implications and give a rounded view of the findings. It is possible to build in a discussion of the pros and cons behind management's current position and whether there are realistic options that may be considered.

A framework for the recommendations It is possible to set the boundaries within which recommendations will fall. Audit recommendations should flow from this process. Hopefully, not only will the audit view be professionally based but it will also be derived from a systematic consideration of relevant material. The types of matters that fall into the change process animated by the report should appear in this, the final part of the ICES.

The aim is to lead the auditor into creative thinking so that problems may be solved. A logical foundation will have been built, which these ideas can be founded on. The ICES will form the main reference document for the wrap-up meeting where material issues will be discussed with the auditee. This working document will also feed directly into the draft audit report in that it will set out what was done, what was found, what it means and what now needs to be done. The stage at which the ICES appears in the report drafting process may be illustrated in Figure 9.25.

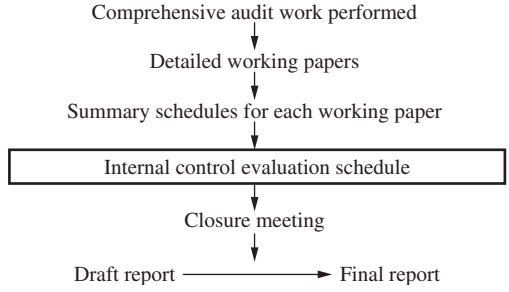


FIGURE 9.25 Internal control evaluation schedule.

The ICES should form a high-level summary of the working papers (properly cross-referenced), which lends itself to being fed directly into the audit report itself. Moreover relevant material, which will enter into the report's standards, findings, conclusions and recommendations, will be found in the ICES that promotes a structured approach to drafting the formal audit report.

Formulating the Audit Opinion

In addition to identifying control weaknesses the auditor is charged with forming and publishing an opinion based on the audit work performed. This part of the audit report may be based on:

The results of control evaluation This will help identify the actual weaknesses that are being addressed via the audit report. As such control evaluation represents the process of establishing the key problem areas in the system under review.

The existing control culture The audit opinion must be set within the context of the management culture. Where there is a fundamental lack of control appreciation, this issue will feature in the report. Where there are sound controls but a lack of mechanisms to ensure compliance, again the audit opinion will reflect this factor. The tone of the report will be geared to the level and extent of change that is required to ensure good control which in turn depends on the management's own perceptions of its control needs. The report can be reconciliatory and highlight all the positive steps taken by management to enhance control, or it may be hard-hitting and seek to get entrenched managers to act on audit recommendations.

Outstanding risk The audit opinion will certainly highlight the implications of outstanding residual risk. These may include, for example, a high level of defined error in the transactions that are processed, inconsistent information that cannot be properly reconciled and/or poor documentation.

The underlying causes of basic problems The audit opinion may operate on two levels whereby the detailed findings will be presented in terms of the type of problems mentioned above. It should also provide an overview where the principal causes may be discussed. In this way, it may be possible to link isolated problems to a common cause. Examples may be a lack of clear procedures, staff absences and/or insufficient segregation of duties.

Whether controls are adhered to This is an important point in that regardless of how sound the controls may appear on paper, the auditor will be able to discover whether they are being applied in practice. The overall results of compliance testing should be referred to in the final audit opinion and if this is a material issue then the relevant facts should be disclosed.

Whether controls work Substantive tests seek to discover the net result of control weaknesses. This should appear in the audit opinion as the level of loss/error/inefficiency derived from residual risk.

The practicalities of available remedies The auditor must look at the available recommendations carefully before presenting them to the management. If a great deal of effort is required to effect any necessary changes then this should be noted in the audit report. Some form of reasoning must appear that justifies the recommended way forward. In some cases, reference may be made to any option that may have been placed in front of management as part of the various audit recommendations. The respective costs and benefits of each control option should be appraised and commented on. The audit opinion will hopefully put this issue into perspective.

Management's efforts to improve Specific improvements should be acknowledged. When dealing with the objectives of the audit report we noted that it is there to provide assurances to management on its systems of internal control. Where management has tackled control problems and put into action improvements, this should be an additional feature of the overall audit assurance. It may balance conclusions and stimulate a positive response from management.

The effects of any future changes planned In formulating assurances the auditor can point to the future by outlining planned changes. This sets a framework for the report. Matters addressed and the auditor's approach to proposed developments should be included in the audit opinion. It enables the reader to judge how far the auditor has gone to relate audit findings to future plans.

Overall impressions on management's ability and willingness to address residual risk We may be dealing with a follow-up audit that uncovers lack of effective management action to address the problems identified in an earlier report. The audit opinion will reflect this barrier to change and perhaps be more critical than the normal tone used. If management has made great strides in meeting problems head-on, then the audit opinion will be directed towards supporting these moves and sympathizing with the management. The net result will vary according to circumstances.

Findings from unofficial sources The auditor may know of problems because staff have reported off the record without providing formal evidence. The 'audit nose' may also have come

to the fore and this may create a dilemma. The auditor may wish to refer to sensitive problems although there is no formal supporting basis that may be quoted. An example is where the line manager for the areas under review is nearing retirement and is not interested in making any major changes. Some argue that the tone of the audit opinion may be altered to reflect unspoken concerns, although this must be used with great care. The CAE should have defined an appropriate reporting standard that will be in the audit manual. The audit opinion is formally communicated and here lies the importance of the tone of the written report. Reporting allows the auditor to convey professional opinion and make suggestions within the context of the management's position.

Formulating Recommendations

It is not enough to point out problems without providing guidance on required action. This is the positive part of the audit report and when formulating recommendations, we should consider:

The available options The audit opinion deals with available options in outline by describing different directions management may take. In the recommendations part of the report this will be dealt with in more detail. We may analyse the options outside the report by assessing them in the working papers. Alternatively, we may set out options within the recommendations. This approach may cause problems where an overload of advice may confuse management and blur the main issues. It is acceptable to give options when performing consultancy services commissioned by management. For audit work, a better approach would be to analyse options in the working papers and discuss these with management at the wash-up meeting before specifics are formally reported.

The need to remove barriers to good risk management and control Some recommendations are based on new resources, some seek to get management to do things differently while others seek to remove underlying problems. Where specific circumstances militate against good control, this needs to be dealt with. The recommendations should therefore take on board control barriers and seek to define ways in which they may be removed. The level of non-compliance with procedure may be related to the extent to which management perceives this compliance as important. A general lack of concern about staff adhering to procedures may act as a barrier to risk management that has to be addressed before we can start considering these controls. Another example of impoverished risk management may be in the form of poor staff that have been employed, despite failing to meet the requirements of the job specification. Again this factor must be tackled before we can have a constructive discussion on control systems. Remember that our wider definition of control takes on board considerations such as sound recruitment procedures. The point is that an underlying foundation that supports good control may have to be referred to before the detailed control arrangements are featured in audit recommendations.

The exercise of creative thinking In many audits, managers are aware of control weaknesses and have noted the implication in terms of errors and/or inefficiencies. They need advice on solving these problems within resources available. The auditor has experience of similar problems and can stand outside the activity to create workable solutions. Creative thinking can be applied in formulating recommendations. This separates the professional auditor from the junior checker. New heights are achieved when the auditor enters the world of lateral thinking with ideas, inspiration and fresh thought. The important ability to associate problems with underlying causes underpins creative thinking. We would expect this exercise of creative thinking to consist of more than repetition of material found in ICQs. One lead into this is to define and assess these associated factors in Figure 9.26.

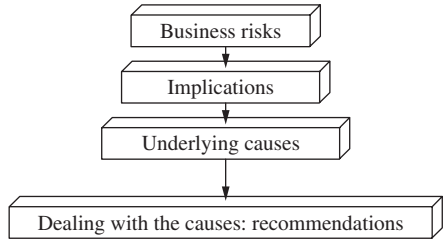


FIGURE 9.26 Searching for recommendations.

Value-for-money (VFM) points The theory of VFM can be controversial in that some writers argue that it is good systems that will promote VFM. Others see an audit as an opportunity to identify new efficiency measures and possibly present a resultant figure for potential savings. The approach will depend on the adopted audit methodology. Where specific savings are being recommended then a level of discussion will have to appear in the main body of the report that justifies the required action. In this case, it may be necessary to build up the actual recommendation itself so that it is more than a one-liner. It is also as well to distinguish these matters from the other audit recommendations that may be directed towards controls perhaps by having them in a separate part of the recommendations.

The resource implications of recommended controls It is possible to indicate the cost of recommendations. So that the report does not raise more questions than it answers. This point is particularly relevant in a recession where new funds are not readily available. This feature need not be exaggerated to a great extent since management clearly has a role to play in assessing and taking on these recommendations. What needs to happen is that the report should acknowledge the fact that it may be necessary to secure additional funding to get improved controls. One way is to seek to minimize the need for actual new resources by setting the recommendations within this context.

An operational area consisted of three teams dealing with accounts by splitting the alphabet between them. A fourth temporary team had been employed to clear up backlogs. The manager had intended to assimilate this new team into a fourth team and spread the alphabet into four sections. A new computer system recently installed was causing disruption and contained poor and incomplete data. Operational procedures were inadequate and staff used inconsistent working methods. A key recommendation was to establish a quality and control team to support the computer system, formulate procedures and promote quality standards. This proposal was sold to management by using the temporary backlog team and transferring some of the duties of the three alpha teams to this new quality team. New resources were not required, it simply involved a change in direction for the current staff.

One of the key flaws in audit recommendations centres on the assumption that control needs will be fully resourced by management. It is flawed because it fails to recognize the tremendous strain on resources that faces all organizations and all sections within these organizations.

Any bad management practices that impair control It is rare for audit reports to contain attacks on management and this approach sets up confrontation. It is essential that audit concerns

are properly noted even if these include poor risk management practices. It is possible to do this in a constructive way that does not bring personalities into play and with careful drafting, an appropriately worded recommendation may be formulated. One factor that impairs control is distant managers who fail to communicate with staff. Problems such as this may be dealt with by ensuring that the recommendations have a good chance of being implemented. We can suggest that managers issue the audit report to all staff and establish regular meetings to deal with the required changes. Where it is clear that managers are not acting as change agents then we can suggest that extra responsibility is given to a defined person to bring about recommended change. In terms of designing new systems (a role outside the audit remit) we may ask management to bring in a consultant where it is obvious that this task cannot be performed in-house. Much depends on the circumstances, and the extent to which audit needs to guide and direct management in its search for better controls.

The ideal solution The section on control evaluation addresses the concept of the ideal control system. This may be established to set a standard that may be aimed at over time. An example of an ideal would be to establish a fully automated operational process and convert staff areas into networked computer workstations. We would not expect recommendation to be too futuristic in that they are programmes to be applied over a long time period. There are some matters that can only be dealt with in incremental stages. Where there is a mismatch between skills required by management and staff and those that they actually possess, we can only seek to achieve so much through audit work. Far from being a solve-all situation, an audit is undertaken to leave the operational area in a better position in terms of suitable control systems. There is no definitive solution that can emanate from the audit report, and this is not the main objective of an audit. The ideal solution will be contained by the real-life practicalities that face all organizations.

The costs of poor control Recommended controls are put forward on the basis that the cost of risks, which they are meant to remedy, outweighs the cost of these new/improved controls. When designing suitable recommendations it is as well to consider this side of the cost equation by reviewing the implications of any lapses in control. It is a test that each recommendation will have to pass if it is to make it to the audit reporting stage. What makes this equation difficult is the view that 'costs' encompass all negative influences that face the area under review, which includes qualitative factors such as general reputation. The actual 'cost' of a poor reputation within the organization may be the closure or contracting-out of the particular function.

Practical workability It is a failing of many auditors to make impractical recommendations. This 'walk away' syndrome means that the auditor is satisfied to perform an audit, make numerous recommendations and then depart, blaming management for not taking a serious interest in the audit work. This can become dangerous where the auditor argues that management has something to hide. It may be that audit performance indicators are based on the number of recommendations made in published reports. The audit process must be accompanied by suitable audit standards that ensure this task of assessing the workability of recommendations is undertaken before they are put forward.

The auditor should point management in the right direction and stimulate effective management action. It is possible to adjust the tone of audit recommendations and choose from:

- We recommend . . .
- We strongly recommend . . .

- It is advisable for management to . . .
- It is essential that management . . .
- Management needs to urgently address . . .
- Management should consider . . .

Auditors may make many recommendations and these should be structured for maximum impact, the most important first. There should be a few enabling steps that management should take and these should be detailed in the opening part of the recommendations. They should be designed to place management in a position to effect the various recommendations. This would also appear in any executive summary and should not consist of more than two or three items in discussion mode. The remaining recommendations should follow in order of priority (see the section below on change management). One useful approach is to document a series of recommendations for each main section of the report and then repeat them as the final part of the executive summary (cross-referenced to the main report). Recommendations should be presented to create maximum impact. There are many busy executives who are primarily interested in what is being recommended, and why.

The Review Process

Audit work should be reviewed before a report is published and this should occur on two levels. First, there should be a supervisory review of the underlying working papers where all audit findings should be supported by sound, evidenced audit work. The second level concentrates on the audit report and the way the work, conclusions and recommendations are expressed. The review should look at the quality as well as quantity of work. If work is reviewed as it progresses the draft report will not be delayed awaiting the audit managers' review. The report review may look for:

The structure The report should follow a defined format and reflect what may be called the house style. A major short-cut to report drafting is to follow an agreed structure. If this has been automated (i.e. held on computer disk), one may imagine the ease by which the outline can be tailored for the particular report in hand. The review process should look for compliance with this standard and seek explanations where it has not been applied.

What the findings are based on There should be a clear link between the terms of reference, the work carried out, the findings and the recommendations. The review will consider the appropriateness of audit findings expressed within the report. The draft report should be cross-referenced to the working papers and particular attention paid to factual quotations placed in the report. These should be accurate and represent sound evidence. Where a fact has been derived from an interview and not confirmed elsewhere, then terms such as 'we have been advised by management that . . .' may be used. The importance of reviewing the findings cannot be overemphasized and the audit manager will have a major role in this respect. As such, the review process cannot simply involve the report but must delve into the working papers themselves. This will consider the way the work was done, the extent of coverage, and the results of the tests applied. The working papers should be able to contain all this material in a simple and clear fashion. One useful test that can be applied by the audit manager is to suggest that it should be very easy to find supporting papers for each key point made in the report. If this is not the case, questions must be asked.

How they are expressed Securing good findings is one consideration but the way they are presented is a separate matter. A major failing for some auditors is to exaggerate the findings or make generalized comments based on very limited information. The scale and significance of evidence uncovered should be properly reflected in the report and, as well as not suppressing major findings, one must also be reasonable in dealing with less material matters. The art of setting the findings within the context of the entire operation that has been reviewed is a difficult one to master. Reports that spend much time referring to a series of minor errors will make very boring reading and can lead to accusations of bias from the client. There is nothing wrong with using specific examples to illustrate a key point along the lines: 'we found several instances where documentation was incomplete and in one case missing altogether'. At some stage, however, we would expect a summary of findings to appear that places our research against the entire population, using percentages where necessary. Such material would be presented along the lines: 'over the hundred items examined, we found that around 15% were not authorized. Some 7% contained errors that would affect the resultant figures submitted to head office, to the extent of £*x*'. If statistical sampling had been applied we can go on to quantify the implications for the entire database.

The tone of the report One important review point relates to the way the auditors have expressed their findings. The reviewer should aim to take out all emotive aspects of the report including underlining, exclamation marks, sarcasm, slang and other unprofessional techniques. This could be a sensitive part of the review process and the reviewer should ensure that time is set aside so that these points can be properly discussed. One should also aim at eradicating unacceptable drafting habits in future reports by explaining their use (or misuse). Internal reports are particularly susceptible to emotive drafting and it can be very embarrassing where these reports are eventually read by outsiders. It is best practice to stick to the policy of saying what needs to be said in a clear and concise fashion using standard terminology, so the problem of trying to read between the lines need not arise. The current trend is to give a degree of passion to the report so as to excite the reader by the use of terms such as 'it is unprecedented . . . , we have a fundamental concern over . . . , management have clearly misdirected their efforts . . . , this is the worst case to come to our attention', and so on. This is an unwise position to adopt as each report competes with the previous one to be more dramatic, until they read more like tabloid newspapers, using a series of clichés. We must restate the view that auditors should resist this temptation and stick to the usual format whereby sensationalism is avoided.

Gaps The report must be read as a whole by the reviewer and obvious gaps isolated. This may include items in the terms of reference that have not been dealt with and findings that do not flow from the work carried out. The key here is to spot where the report leaves too many unanswered questions that lessen its overall impact. Where the report has been written over a period it may appear disjointed with repeated points and areas that have simply been left out. If one part of the report states that an issue will be expanded on, later on this should happen and a relevant section added to a later part of the report. If we have decided to restrict the terms of reference for an audit and leave one component to be covered in a separate audit then we must say so. We cannot assume that the report writer will always be available to explain apparent inconsistencies, which means that the report should be read as a complete document now and in the future. Gaps in the report will tend to annoy the reader, particularly where specific items have been left out with no explanation. Where, for example, we have found a major error, we must indicate whether management was made aware of this immediately and whether the matter has been put right and any losses recovered. To do otherwise would leave the reader in the dark, with many unanswered questions.

The terminology used The auditor is faced with a dilemma at times where, although the line manager will be the main client for the report, it will also be read by others less familiar with the area under review. As such, it is important that all terms used are explained and a list of abbreviations appears in the appendices. It is best to apply the policy that a report should be understood by all potential readers, and if audit is working to the highest professional standards then we would expect the chief executive, and top management to take an interest in our work. These senior officers will tend not to have an intimate knowledge of all operations, which means that audit reports should not be written only for operational management or technical experts. Excessive use of abbreviations may make a report incomprehensible.

Spelling and grammar This is a material point in that many audit reports contain excellent findings and crucial recommendations but are let down by poor spelling. This distracts the reader from the important points being made by allowing them to fall into a mode of active criticism whereby they look for further mistakes in the report. All word processors have grammar and spell checks and it should be a standard that no work is prepared without using this facility.

Whether the house style has been applied Titles, colours, logos, binding and report covers should all follow the adopted format. Draft reports could be prepared to a lower presentation than the final versions which may be bound in expensive covers. If final reports have different colours then they will be distinguished from drafts. If there is, in fact, no house style then the CAE may be open to criticism as reports are published in an assortment of ways that do not promote a corporate view of the audit function. One simple standard is to set a procedure whereby different covers have been defined, for example:

White – internal use only
Pale green – all draft reports
Pink – confidential reports
Dark green – final published reports

Whether it appears as a professional job well done The reviewer should ensure that the report reflects a well-done audit that has directed itself to the terms of reference. The overall 'feel' of the report should be in line with audit standards and this is something that is achieved over time as the auditor becomes more and more experienced. If this test is not satisfied, then the reviewer needs to go through the draft in greater detail so that it can be improved. It is always a good idea to read a report as a whole document and not as a series of separate sections to gauge this overall impression. We would look for this balance that recognizes what we have found, what management is doing, where it needs to go and so on, so that the document reflects a considered view of the systems that have been audited. There are times when a fresh eye is needed to make this decision, removed from those who have been intimately involved in preparing the report.

Whether the client would be quite happy to pay for the resources invested in the audit One interesting feature of the review will be to ask whether the report is worth the cost in terms of audit hours. It is good practice to cost out audit hours so that audit management may then pose, for example, the following question:

> Does this report represent £10,000 worth of audit work?

Again it is practice that allows us to make this judgement in terms of VFM. The old adage of 'Assure, Alert, Advise and Action' is foremost in this consideration where we deem our role as assuring management that all is well. If not we would alert them to any particular problem and

then furnish some degree of advice to assist them. The report must offer this format in the search for added value from the audit service.

The Clearance Process

The draft audit report, once reviewed, has to be cleared and management given the opportunity to comment on the contents. The findings should not come as a surprise to management and it is advisable to bring them to the manager's attention as they arise. Regular progress reports (probably oral) and a brief meeting at the end of each week will assist this process. A wrap-up meeting with the line manager should be held at the end of the audit where the main findings are discussed. The reviewed draft should be sent to the line manager (only) and an informal meeting held to discuss this as soon as possible after completion of the work. Factual matters should be dealt with and the auditor may well revise the draft as a result. The auditors' conclusions will only change where the factual corrections materially affect audit findings. Once this has occurred, a further draft should be formally sent to those affected by the work including the next tier of management. Formal written comments will be taken on board and a final report published. This is a useful technique for involving the actual operational manager as the report will be more reliable and we would have hopefully secured this officer's full support before it goes to a wider audience. Note that where management accepts without question all audit recommendations, this may mean they are not particularly interested in the results and wish to get rid of the auditor. Effective action normally starts with close discussions with management on each audit recommendation. Again see the section below on change management for a different perspective on this issue. Management is entitled to choose not to follow audit recommendations and in this instance it is the auditor's responsibility to ensure they understand the implications and are prepared to assume the associated risk. Management will then assume full responsibility for this documented decision and this issue may be brought to the attention of the audit committee.

Formulating the Action Plan

It is a good idea to form an agreed action plan with management based on the audit. This allows management to take over the audit recommendations and so be fully involved in implementing them. An action plan may be devised during the drafting procedure and once agreed may be included in the published report. Where management is allowed to form its own action plan, this becomes a very efficient way of getting audit recommendations implemented, although we would expect a degree of negotiation by both sides. Accordingly the auditor should work out which recommendations should be pursued and which may be partly given up for a greater good. The best solution is to include the action plan within the executive summary as part of the agreed solution and we would look for items such as work required, by whom, deadlines and reporting lines as a way of ensuring that the recommendations will come about. Once complete, the action plan should belong to management as it seeks to embark on the necessary workload.

Supportive Evidence

Recommendations must be based on sound evidence and the extent of this supporting material depends on the importance of establishing the effects of control weaknesses. Where internal

auditors are required to attend management working parties which publish reports and make recommendations without comprehensive research then their views should be qualified as not being derived from the normal audit process. The formal audit reports in contrast must be based on sound evidence that has been derived from the audit process.

Change Management

Many auditors become demotivated when their audit reports are more or less ignored by the client. Some feel that line managers should be disciplined through failure to act on audit recommendations while others simply feel less enthusiastic about their work as a result. Where reports are not actioned there is always an underlying reason. Occasionally this is because management is acting negligently and against the best interest of the organization. More often, it is because they can see no good reason to obey unrealistic recommendations made by people who do not understand the operation in question. Audit recommendations generally form part of a change process in that they tend to ask for something that is not already being done. As such they lead to some of the tensions that change itself creates and this in turn affects the client. Moreover, the auditor may also be a source of management stress. When performing an audit the auditor should recognize the implications of the change process and ensure that where necessary these are taken on board particularly at the reporting stage. The chapter on behavioural aspects of auditing provides further insight. At this stage (there is a separate chapter on change management) it should be noted that on receipt of a draft audit report the client may exhibit some of the following reactions:

- What does this mean?
- Will I lose out?
- Will I benefit at all?
- How should I play this?
- Will this lead to something bigger?
- Can I use this to get something?
- Is the auditor manipulating me?
- Is there a hidden motive behind all this?
- What are the costs of getting these recommendations actioned?
- Can I afford to ignore this report?
- Will my boss support me?

Where these questions are left unanswered, the client may feel threatened and react negatively. If the audit has been professionally carried out with a clear understanding of management's systems objectives along with its close involvement at all stages of the review, then these fears may be reduced.

Logical Presentation

The flow of information contained in an audit report should follow a logical path that takes the reader through the audit process itself. The logical flow may appear as in Figure 9.27.

There are many ways that this information may be presented, although the principle of providing a logical flow of problems, causes, effects and required action should stand.

Subject

Scope

Planned cover

Actual cover

Mode

Existing deficiency

Underlying cause

Effect/implication

Enabling structure

Required changes

FIGURE 9.27 Logical presentations.

Structuring the Audit Report

A defined structure for audit reports should be implemented by the CAE and this should be followed when drafting audit reports. This will vary from department to department depending on the nature of the work that is carried out and the type of officers who will be receiving the audit report. One example is in Table 9.7.

TABLE 9.7 Report sections.

Section	*Coverage*
One	This will contain the executive summary to the report.
Two	This will outline the objective, scope, approach and work done.
Three	This will contain a background to the area under review.
Appendices	Restrict these to the minimum.

The CAE should adopt a suitable policy on responses from the client and they may be:

- **Incorporated into the report.** Here adjustment is made throughout the report to reflect the comments received from management. A note to this effect may also appear in the report which is a technically correct approach, but can lead to delays in achieving a final draft for publication. There will also be some comments that the auditor does not agree with, and again the way that these are presented will have to be thought about.
- **Built into a management action plan.** The important part of the report is the action plan and it is possible to build management's views into this section without making numerous adjustments to the main body of the report.
- **Included as an appendix.** A convenient method for dealing with responses is simply to include them as an appendix to the report. The problem here is that they may be taken out of context if a form of audit responses to the comments is not included. We may imagine, however, that a continuous exchange of memoranda based on responses to responses could become an embarrassment to all sides and this should be avoided.

Some audit departments send the draft for consultation without the executive summary and formulate recommendations after the client has been able to comment on the findings. The participative approach comes into its own where the auditor forms joint recommendations with the client after discussing the findings. This agreed action plan is then reported in the executive summary. Note that where there has been close cooperation throughout the audit, problems with formal responses will probably not arise.

Ongoing Drafting

Most auditors are very efficient when performing the field work and by working hard can give a good impression to clients. Back at the office, there is a tendency to slow down and spend much time on drafting the audit report and this may lead to delays in publishing the report. One solution is to encourage auditors to write reports as they carry out the audit and the outline structure may be drafted as soon as the audit is started. Laptop PCs are essential to this process and as drafting occurs, any gaps may be spotted before the auditor leaves the client. Where a reporting structure has been agreed via the audit manual then one will be able to complete an outline when the audit is started. The terms of reference part of the report may be drafted from the assignment plan while a section on background to the operation will be available in the early part of the audit. It is not acceptable to produce reports weeks after the audit and the reporting standard should set clear deadlines on this topic.

Good Audit Reports

The previous section dealt with general concepts behind audit reports and Mary C. Bromage has explained what makes a good audit report:

> Clarity and objectivity are long-avowed aims of functional writers including those in accounting. As these two attributes are now carried over into operational auditing, and into management studies in general, additional skills are demanded. The end product of functional writing, a formal report, is expected to be direct, concise, objective, verifiable, convincing, and (what is more) interesting. Such goals cannot be achieved by the amateur, either as writer or as auditor. They depend on the acquisition of techniques in the communication process. Not all students of business necessarily prepare themselves to be skilled in English.[19]

This section summarizes some more features of good audit reports:

1. The client should be thanked for cooperation and assistance through a formal acknowledgement in the report. The auditor must be prepared to rise above negative management attitudes and even if the level of managerial support was not great, the acknowledgement should still be included in the report.
2. The report should normally not name names. One would refer to the designated posts wherever possible. Investigation into fraud and irregularity may be exempted from this requirement. Remember, we are not auditing people; we are auditing systems, procedures and circumstances. This principle also applies to any appendices that appear at the end of the report, where details that identifies people should be removed from tables and schedules. Even where an officer is being commended we would still not wish to mention an actual name.

3. An action plan agreed with the management should be set out in the executive summary. This represents the 'agreements' reached on the basis of the report and passes responsibility for the required changes from audit over to management.
4. We should always balance both good and poor features of the area under review so that we are seen to be fair. Recognition should be given to managers' efforts and any drives they have for improvement should be supported. We must also recognize pressures impacting on management's time and resources. Poor managerial practices may be seen more as barriers to these sought-after improvements, rather than disciplinary offences. If management has started to make changes as a result of an ongoing audit, it is not a question of who claims these improvements, but more a matter of mutual recognition on both sides. Any progress made on improving controls can be mentioned in the report, as well as reporting these changes as formal audit recommendations.
5. The client's views should be reflected within the report or their formal response set out as an additional appendix, to ensure that both sides to the audit have been fairly represented. This is particularly important where some degree of disagreement is present.
6. The whole style of the report should be positive and should not consist of a list of basic criticisms. If an audit is done well then the client will look forward to receiving the report as being a useful contribution to the management task.
7. The auditor should never blind the reader with science by using technical gibberish. This shows a flaw on the auditor's side in an inability to communicate effectively which is wholly unacceptable.
8. All reports should be professionally presented. If an unfinished draft is urgently required this should be quickly followed up with a final formal report that has been completed to professional standards. The first draft should state clearly the status of the document, giving reasons.
9. The report should appear fresh and clear so that the reader might enjoy it. A well-written discussion-based style can assist this process with relevant summaries for quick consumption by busy executives. Factual discussion without recourse to emotive phrases is the best policy as long as this does not become too boring.
10. All facts should be quoted precisely. If part of the findings is based on limited information, or unconfirmed data, then this should be clearly noted. If facts are conclusive then we are entitled to say so.
11. One may wish to use the audit 'we' when describing the audit opinion. This personalizes the work in one way by implying that it comes from the audit department, as opposed to some unseen force. On the other hand, it does not make it too intensive as it would be if it came from one individual (as would the use of 'I').
12. The required action should be set out in a hierarchy of descending importance with the more important recommendations appearing first along with an appreciation of problems that may face management in implementing them. To this end the recommendations should be set within an enabling framework that may be described within the audit conclusions.
13. All excessive detail should be relegated to the appendices. These should be referred to in the report, but will not be essential reading. The operational manager might wish to study the appendices in detail, whereas the director will probably concentrate on the executive summary. For this reason we would wish to see an amount of background information in the report that provides an insight into operational problems facing line management, and so make the report easier to follow.

14. Terms and structures should be consistent and follow logical processes. Where we refer to something in one way in the report, this term should be used through the document. Points made should support each other and contribute to the final audit opinion and ambiguity should be avoided. Various types of ambiguity have been described by Nigel Warburton:
    - Lexical ambiguity – word has two or more possible meanings – for example, discrimination = prejudice or an ability to judge
    - Reference ambiguity – word can be used to refer to either of two or more things – for example, him = which one?
    - Syntactical ambiguity – order of words allow two or more interpretations – for example, small fish packing factory.[20]
15. The work should flow logically with each point building up into a complete picture. Findings represent the culmination of this process. Without being too dramatic it is possible to take the reader through the system and how each part interlinks to form a whole system of internal controls. The reader should be reminded that these controls allow the management to achieve its objectives and failings in one area rebound onto other areas and affect the overall quality of the end product.
16. Reports should be well presented but not too 'glossy'. We should be aware of the notion that the client is in effect financing the audit work and unnecessary waste and extravagance can be criticized. At the same time a final report should appear professional with the audit logo and card covers with cut-out windows, using desktop publishing standards.
17. The report should be client-oriented in that it is directed at the needs of the reader. One useful technique is to use a standardized audit cover, white paper for the main body of the report, a separate colour for the executive summary at the front of the report and another colour for the appendices.
18. Reports should be produced quickly and one would expect the audit department to invest in laptops, laser printers and a report-binding device so that the draft does not spend weeks 'at the printers/typist'. The reports should be produced in-house to professional standards of desktop publishing quality. It is advisable to use an audit administration officer to help prepare the copies.
19. The work should recognize the various constraints that management faces and build these into the recommendations. An understanding of the pressures on managers and the criteria they apply will bring an element of realism to the audit.
20. We should state clearly the objectives, terms of reference and scope of the work and whether these were in fact achieved during the audit. All points on the terms of reference should be referred to in the findings and conclusions. If a participative style is assumed, then this should be reflected in the report, and the 'we' might in fact refer to the auditor's and management's joint efforts. If this is the case then we may not formulate audit recommendations, but instead agree and document a suitable action plan with management. This, however, will depend, in part, on the role of audit in the organization.
21. The report must address the real risks facing the management if it is to have any relevance to organizational objectives. It is best practice to aim at the most material, sensitive aspects of the operation under review and hence direct audit resources at real issues.
22. We must always remember that an ideal position is impossible to achieve and we have to work within the realities of the existing environment.

One fundamental truth the auditor must face is that a good audit report is based on the quality of the audit work and liaison with management that has to be done before one is able to report the results.

Audit Expertise

When addressing the topic of audit reports it is vital that the auditor understands the actual role of audit. Managers are responsible for their operations and they will retain this right long after the auditor has done the review and departed to new fields. There are several points that should be mentioned to draw out this important concept:

1. Auditors should never assume that they know more than management about the particular operation. They are not paid to be experts in any one area. The auditor brings to bear an experience of controls and how these might be evaluated and tested. A 'know-it-all' stance is off-putting and can only lead to problems when reporting the results of the audit. The audit must start from management's perspective and what it is seeking to achieve from the operations. The audit task is to feed into this process and examine the controls that have been provided to support the operation. What works in one organization/department will not necessarily be appropriate in another and it is here that the auditor must be very careful. The report must be drafted in line with this principle.
2. Audit is not there to 'prop up management' and if it assumes this role, management will continue to require this service while the organization will suffer. Assume management operates a substores that holds local supplies that the central stores would take too long to provide. Management asks for an audit of these stores and it becomes clear that it knows little about this unit. Audit then reports on the numerous problems that exist because no controls have been established whereupon management requests an audit and stocktake every six months. Audit is covering for management's failure to control the stores and the auditor's regular presence perpetuates this failing. A more common example is where management fails to define clear access procedures for computerized systems. They refer numerous cases of systems breaches to audit for advice on any action they may take against the employees. As long as we provide this service, management need not bother to plan and install suitable controls.
3. Audit is not employed to solve minor managerial problems since audit resources must be directed at material high-risk areas. Constant fire-fighting perpetuates the situation, particularly where resources are not available to deal with material control implications. Where audit responds to systems that have broken down without encouraging management to establish sounder controls this fire-fighting mode will continue. Audit may appear busy solving management's problems but this is a misdirection of resources.
4. Audit should not feel that it needs to show managers how to do their job. If management is unable to perform, then this is a control deficiency that needs resolving.
5. Audit should not second-guess management. If management does not know what it is doing, then the underlying causes must be addressed. There are many ways that services/products may be delivered and audit need not assume an executive role in this respect.

As the audit role moves away from inspection to consultancy the question of expertise will become increasingly sensitive. Computer specialists, human resource managers, engineers, quantity surveyors and so on are now employed in the audit department. Despite this trend, it should be made clear that audit is, above everything else, expert in control. The recommendations in the audit reports will reflect the relationship between audit and management and it is essential that these concepts are carefully portrayed in the way the audit report is drafted. The point is that audit must decide what it wishes to achieve before it can communicate these concerns in a formal audit report. If our role is to 'check up on management' then so be it as long as this is a conscious decision rather than an individual auditor's whim.

The One-Minute Manager

Research has shown that a typical manager will spend only a few minutes on each item of business before turning to another matter. Auditors who cannot identify with this point will find their work for all intents and purposes ignored. Managers may speak of the 'audit books' to describe the detailed reports sent out by the audit department that are full of what appears to be insignificant facts and endless testing results. In addition to using executive summaries, the auditor is well advised to give oral presentations to bring home audit points and in so doing save management much time and effort. The manager may need quickly to know:

What is the problem?	What caused the problem?
What are the implications?	What is the best solution?
What action should I take?	What happens if I do nothing?

An auditor who anticipates and answers all of these questions in, say, a brief meeting/presentation will be well received by senior management. Note that the formal comprehensive audit report should still be provided. The key is to anticipate unanswered questions and resolve them. If this does not happen then the impact of the audit report is lessened and a tendency not to act on the findings will arise. One only makes changes where there is a clear impetus based primarily on sound justifications and clear benefits. The realities of working life mean that management does not have time to deal with anything that fails this basic test. The audit manual should contain a specimen audit report. Having this on disk assists preparing audit reports and saves time. It may be necessary to have a number of specimens for short reports, for longer ones and for reporting the results of fraud investigations. Another useful standard is to insist that each paragraph in the report is attached to a unique paragraph number from one onwards, for ease of reference. Practice Advisory 2410-1 (extracts only) gives some sound advice on audit reporting and possible communications criteria:

> Although the format and content of the final engagement communications varies by organization or type of engagement, they are to contain, at a minimum, the purpose, scope, and results of the engagement.
>
> Final engagement communications may include background information and summaries. Background information may identify the organizational units and activities reviewed and provide explanatory information. It may also include the status of observations, conclusions, and recommendations from prior reports and an indication of whether the report covers a scheduled engagement or is responding to a request. Summaries are balanced representations of the communication's content.
>
> Engagement observations and recommendations emerge by a process of comparing criteria (the correct state) with condition (the current state). Whether or not there is a difference, the internal auditor has a foundation on which to build the report. When conditions meet the criteria, communication of satisfactory performance may be appropriate. Observations and recommendations are based on the following attributes:
>
> ***Criteria:*** The standards, measures, or expectations used in making an evaluation and/or verification (the correct state)
>
> ***Condition:*** The factual evidence that the internal auditor found in the course of the examination (the current state). Cause: The reason for the difference between expected and actual conditions.

> ***Effect:*** The risk or exposure the organization and/or others encounter because the condition is not consistent with the criteria (the impact of the difference). In determining the degree of risk or exposure, internal auditors consider the effect their engagement observations and recommendations may have on the organization's operations and financial statements. Observations and recommendations can include engagement client accomplishments, related issues, and supportive information.

IPPF standard 2420 on the quality of communications states:

> Communications must be accurate, objective, clear, concise, constructive, complete, and timely.
>
> *While the i*nterpretation explains this concept:
>
> Accurate communications are free from errors and distortions and are faithful to the underlying facts. Objective communications are fair, impartial, and unbiased and are the result of a fair-minded and balanced assessment of all relevant facts and circumstances. Clear communications are easily understood and logical, avoiding unnecessary technical language and providing all significant and relevant information. Concise communications are to the point and avoid unnecessary elaboration, superfluous detail, redundancy, and wordiness. Constructive communications are helpful to the engagement client and the organization and lead to improvements where needed. Complete communications lack nothing that is essential to the target audience and include all significant and relevant information and observations to support recommendations and conclusions. Timely communications are opportune and expedient, depending on the significance of the issue, allowing management to take appropriate corrective action.

Audit reporting procedures play a crucial role in the success of audits. The reporting mode should be geared into the culture of the organization and the needs of management. We have set out the minimum information that the auditor needs to consider when acquiring expertise on communicating the results of audit work as required under audit standards. We should also refer to the internal audit department's own reporting standard which will reflect the audit role agreed with the organization.

The Art Of Expressing An Internal Audit Opinion

By Dan Swanson, *Compliance Week Columnist*

Executive management, audit committees, and the board want to know whether their internal control systems work. The chief audit executive is often requested to issue an opinion on the adequacy of internal controls within the organization to meet this assurance need. If a CAE does issue a formal opinion, it's crucial that all parties clearly understand the areas and issues the CAE is addressing in doing so. Otherwise, brace yourself for expectation gaps. Expressing opinions is no easy task. The CAE must consider the scope of the audit effort and the nature and extent of auditing performed, and evaluate what the evidence from the audit(s) says about the adequacy of internal controls. A formal audit opinion should clearly express four points:

1. The evaluation criteria and structure used;
2. The scope over which the opinion applies;
3. Who has responsibility to establish and maintain the system of internal control; and
4. The specific type of opinion being expressed.

Extensive Planning To Express An Opinion

In planning the opinion, internal audit needs to understand the current ''maturity'' of the internal audit efforts and where the organization is in its efforts to implement a robust system of internal control. Some key questions to consider include:

1. Has the internal audit function evaluated the system of internal control previously?
2. How well-documented, stable, and understood are the organization's controls? (Expressing an opinion is much easier in an organization where statements and management assertions about internal controls already exist, since the auditors can examine the processes underlying the statements and assertions to form their opinion.)
3. Has this evaluation been discussed with the board of directors?
4. How accurate is the disclosure to your shareholders and other stakeholders?
5. Have there been adverse opinions by the external auditor?

In addition to the maturity of the internal audit effort and maturity of the organization's system of internal control, a third dimension must also be considered. That is, at what level of internal control is an internal audit opinion required? The initial SOX-initiated internal control evaluations often covered thousands of controls, which took an inordinate amount of audit time and resources. A lesson learned was to scale back and be more selective regarding the controls to be evaluated. This is a crucial scoping decision; rather than jumping into an examination of a vast number of controls, a SOX lesson has been to focus on the ''key'' controls. In practice, the burning question now is exactly what the key controls are. This can only be answered in reference to the purpose being served by the internal audit opinion. What do the users of that opinion want and need?

The audit department has to consider the reality that an organization with evolving internal controls will need considerably more time and effort to identify, test and assess controls than one with stable and well-understood controls. It may also make a difference in the caveats that should be placed on the internal audit opinion. In fact, an important message has been that depending on your starting point – especially for many internal audit shops not yet providing an opinion at the ''organizational'' level – it will take multiple years before you have enough work and knowledge to provide an overall opinion. The issue of gathering sufficient information from all significant areas of an organization – compliance, disaster recovery, environmental, risk management, governance and internal control – to form an overall opinion is very daunting (read: amazingly labor-intensive).

Communicating The Results

Assuming planning was effective, expectations were clearly set, and audit testing was sufficient to support an opinion of some type, when internal audit communicates its opinion on the system of internal control there is still much to consider in issuing the actual opinion, including:

- **The evaluation criteria used must be clearly stated: what control model was used to complete the opinion, or even just what standards were used to form the opinion**. Complications always exist. For example, the COSO model is most often used to evaluate the overall system of internal control, while the COBIT model is commonly used for general IT controls. The internal audit and the IT audit efforts both need to contribute to the overall audit opinion regarding the system of internal control.
- **The scope over which the opinion applies must be clearly communicated in the opinions document**. What areas of the organization are covered, what work was completed, and what period is involved, are all examples of the issues that need to be covered within the scope statement. An opinion with a well-defined scope will not leave the reader guessing as to the relevance and focus of the opinion, nor the time period to which it applies.
- **Who has responsibility for the establishment and maintenance of internal controls**. Here the issue is ensuring that management's responsibility for internal controls and the board's oversight regarding the system of internal control are both clearly stated. Internal audit is to provide assurances regarding the performance of controls and the system of internal control, but it should not take on any management responsibilities for internal control.
- **The specific type of opinion being expressed by the auditor**. There are varying levels of assurance possible regarding internal control opinions, as well as both positive and negative assurance opinions. Fundamentally, negative assurance indicates nothing came to the attention of the auditor during the audit, while positive assurance indicates the auditor has performed sufficient testing so that the auditor believes it is very unlikely that anything materially wrong is occurring. Here, the issue is audit workload; more assurance means more work. Also, while the CEO and CFO can certify that their financial statements and the processes to create them are accurate, the senior executives are responsible for these processes. Internal audit needs to complete enough audit work to provide sufficient support for its opinion, which is something quite different.
- **Other considerations**. There are always other issues to consider and usually these are situation-specific. Be forewarned that expressing an opinion on the system of internal control is complicated and a long-term proposition. Also, like so many other complicated things, the third time you've completed it, it'll finally fall into place.
- The assurance needs of the audit committee and management are very similar, but they do differ. For example, fundamentally the board wants to know that the overall system of internal control is robust and working effectively and reliably. While this is important to management, executives also want to know what significant improvement opportunities exist, and how they can make the organization more cost-effective. Internal audit needs to balance the assurance needs of both these audiences, and deliver on both.

An extensive discussion between all the key parties upfront is crucial, as setting clear expectations and the overall goals are absolutely required. As the old expression goes: ''Plan your work, and work your plan.'' This definitely applies to audit opinions.

Reprinted from *Compliance Week*. This article was originally published in Compliance Week. Reproduced by permission of Compliance Week. All rights reserved.

9.9 Formal Presentations

From the previous section, it is clear that oral presentations of audit reports can be great successes that lift the profile of the audit function, or they may be total disasters. They have to be managed and, assuming that a positive atmosphere has been established, we can refer to the work carried out by Steve Mandrell[21] who suggests that one can address this subject on four levels:

1. Anxiety
2. Preparation
3. Visual aids
4. Conducting the presentation

Anxiety

The starting place for would-be presenters is to determine where one is located (in respect of oral presentations) on the scale in Figure 9.28.

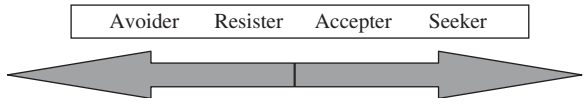


FIGURE 9.28 The anxiety scale.

In other words, an individual may enjoy and seek the task of performing presentations or, at the other extreme, avoid them altogether. In the middle fall those who will do them if pressed. Once the position has been identified then the required level of development can be determined. The impact of a good presentation is crucial in securing support and action. The fallout from a poor presentation could lead to tremendous problems. These differences were starkly described by Alan Baldwin, drawing on examples provided by Edward Tufte (professor at Yale University):

- **Good presentation:** In the US in 1987, John Gotti was acquitted of Federal racketeering and conspiracy after a seven-month trial. A fundamental weakness in the case was the prosecution's reliance on evidence from criminals. This was brought home to the jury by a simple chart. Written across the top were the names of seven principal prosecution witnesses. Down the left hand side of the chart were listed 69 crimes, including murder, heroin possession and sale, and pistol whipping a priest. Finally, the chart was marked with thick black crosses indicating which crimes had been committed by which witnesses. The resulting forest of black marks persuaded the jury not to rely on the evidence of those witnesses.
- **Poor presentation:** In 1986, seven astronauts died when the space shuttle Challenger exploded shortly after its launch. Two small components – rubber rings – in the craft leaked. They had lost their resilience because of the very low temperature that day. The day before, the engineers had opposed the launch. They had faxed 13 pages of information to NASA to support their worry about the stability of the rings when cold, but were unconvincing. In Tufts view, they should have shown the whole history of ring failure, they should have given different weightings to the different degree of damage and shown evidence relating to the temperature when the launches were made . . . they should have explained that in launches above 75°F there was no problem but at 53°F significant problems resulted. The fatal launch was made at a temperature of some 29°F.[22]

On the topic of ensuring the presentation is well planned and delivered, the following should be noted:

Preparation is the key to success Where the auditor is comfortable with his/her material, we would expect a better performance. Not only does this engender greater confidence but preparation also makes sure all important matters have been considered and built into the presentation. This policy has a practical application within the audit unit, in that it depends on sufficient time to make arrangements for the event. Audit management and the CAE should encourage this, and view time spent developing acetates, setting up equipment and so on, as part of the legitimate chargeable time for the audit.

Practice makes perfect Following on from the above, one factor that tends to lower the overall level of anxiety is a foundation of past experience that should make each presentation easier. This consideration relates to previous presentations and also going through the motions of the current one beforehand. Trial runs enable one to time the event and iron out parts that do not readily flow. They also instil a sense of ease as the auditor has to now repeat what has already been performed (as a practice run) rather than undertake a completely new experience. We can bring in a volunteer auditor to assess the practice run or, more appropriately, the audit manager should sit in to gauge the way the auditor performs.

Eye contact with the audience is essential Some nervous reactions are based on a fear of the audience who are perceived by the auditor as a potentially hostile group. To see the audience as individuals breaks down the conspiracy theory and it is through eye contact that this is made possible. The art of making contact naturally without fixing on any individuals should be practised by the auditor in the run-up to the presentation.

Muscle tension can be reduced This is where the muscles are purposely tensed then released. Being aware of our muscles is a step in the right direction. Anxiety causes tension that can be translated into muscle tension, normally preparing the body for a state of alertness which militates against a relaxed state. Most presenters will tend to be nervous although this will be at varying states in line with the level of resistance/acceptance (as indicated in Figure 9.28). The idea is to stop these nerves from interfering with the proceedings.

Breathing should be deep This helps relaxation and so allows the words to flow more freely. This is linked to the earlier point on muscle tension where poor breathing, because of anxiety, can interfere with the flow of words from the auditor. Trying to control breathing, by being aware of this problem, can help in solving this problem. This awareness is heightened by exaggerating our breathing and then bringing it back in control, as a technique applied just before the event.

The presenter should move around slightly This releases tension, although we should not exaggerate this action. Nerves can interfere with the smooth flow of information, which in turn can result in the delivery collapsing. The worst case is where the auditor feels tense, stands very still and starts to retreat into him or herself. Moving around from side to side in a considered manner not only brings all section of the audience into the proceedings but also contributes to relaxation.

The presenter must know the subject well The auditor must have a detailed knowledge of the audit. It is better for the field auditor to perform the presentation, perhaps after an introduction from the audit manager. One feature that makes the presenter more comfortable is the ability to refer to examples to illustrate points. While most of these can be prepared in advance, there are some that will flow from discussion as the audience become involved interactively.

One may visualize the presenter's role and the objective of getting a message across Anxiety is based on a perception of oneself as the centre of the universe, where all eyes are set on the presenter. Where we are able to shift the focus from oneself to the subject at hand, we will perform the role of facilitator. By concentrating on the message, we may not have time to think about being nervous.

The above is concerned with reducing nerves and increasing relaxation so that the auditor may perform the presentation free from self-generated barriers. One of the key factors in a successful presentation is enthusiasm where the audience can be captured and the auditor acts as the change agent in terms of improved controls. This enthusiasm can feed from nervous energy and to an extent we may seek to encourage some adrenalin. We may construct a cycle to take this on board in Figure 9.29.

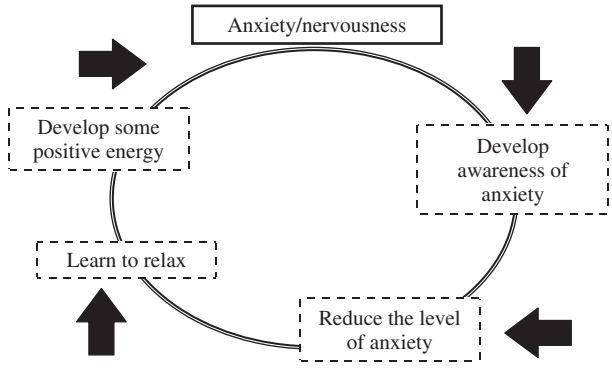


FIGURE 9.29 Managing anxieties.

The idea is to manage anxiety by recognizing and controlling it, rather than removing it altogether as a way of enhancing the impact of the presentation.

Preparation

We have referred to adequate preparations as a key requirement and this will involve:

Notifying the various parties in good time We will wish to invite the line manager and senior staff in the areas to attend. Anyone missed out will probably deem this to be a conscious decision and, to avoid embarrassment, we must ensure that invitations are properly issued.

Setting a clear audit objective For our purpose we will wish to present the results of the audit so as to introduce the draft audit report that will then be made available. It will not be to fully clear the report in detail as this will be impossible to do 'on the spot'.

Organizing handouts Matters that will be referred to that cannot really be included in slides should be given out in advance, or made available at the start.

Using visual aids These should be firmly in place in preparation for the presentation. The main problem is that the various devices such as a PowerBeam and laptop may have been lent out to other sections. We would also want to test any such equipment beforehand.

Selecting a series of examples that may be used to illustrate specific points These should be taken from the audit and should consist of findings that were derived from testing. The audit standard that requires findings to be supported by sound evidence should also be applied in the presentation format. Charts and tables make ideal presentation tools as acetates.

Administrative arrangements so that delegates are not inconvenienced Coffee, biscuits, maps, handouts, seating arrangements and other administrative matters should be part of the preparation. A suitable checklist of items for consideration and action assists, as would an audit administration officer who is able to work at the highest levels.

Time should be carefully planned and rehearsals help clarify this At the start of the presentation it is a great benefit to be able to give an indication of how long it might take, so as to provide some form and structure. Once set we should try to stick to the time frame.

The level of technical competence of the audience should be determined and the presentation format directed accordingly The managerial level should guide the detail provided. It is useful to go through a dress rehearsal in front of an audience with constructive feedback. To get a message across one suitable format appears as: Introduction, Work carried out, Findings, Conclusions, and Next steps.

Visual Aids

There are many techniques that assist the presenter and turn what may be a very boring affair into an interesting and enlightening session.

Visual aids include:

- Dry wipe board. Remember to avoid the most common mistake of using permanent pens on the dry wipe board.
- PowerBeam – computer-based slide presentation system.
- Overhead projector with spare bulbs.
- Handouts that are linked to the acetates.
- Flip charts on a separate board where permanent markers may be used.
- BluTak can be used to put up charts and standing data to be constantly referred to. With a list of material that will be covered during the presentation, it is as well to put this up with BluTak (a sticky substance for binding papers to the wall) and tick each one as it is dealt with.

Visual aids should be used with care and here is some relevant guidance:

Use a pointer to highlight specific items that are being spoken about on acetates It is good practice to face the audience when speaking, which means it is better to refer to the images on the overhead projector rather than the screen.

Any slide should be carefully designed to provide attractive images Professional standards require that they should hold the attention of the audience and may include sound graphics and moving images.

Use the illustration to focus attention Never fill the presentation with excess information or a copy of a detailed document. Slides should contain checklists or key pointers to expand on during the presentation. One approach is to use cartoons to pick up on key points. Humour should be used with care as we would seek to use neutral subjects that will not offend any section of the audience.

Watch the positioning of equipment so that all can see There are many presentations that leave parts of the audience in the dark because of obstructions that block vision. A quick check from each side will make it clear whether there are obstructions. There are times when the presenter will have to move across the room and provide brief apologies. If the presentation is crucial, lights in the front of the room may be dimmed for greater illumination.

Do not overload the audience with information and tables Some matters can be left for later consideration when the draft report can be read at leisure. This should be made clear during the presentation so that items such as schedules of errors found can be addressed at a later meeting.

Conducting the Presentation

The physical environment for the oral presentation may be illustrated in Figure 9.30.

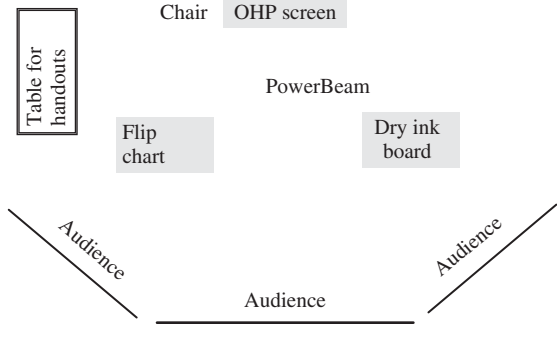


FIGURE 9.30 The presentation's physical environment.

Practical considerations when conducting the presentation are:

Anticipate questions and ensure full answers are provided Some auditors see questions as flash points where possible confrontation may arise. The usual motive for questions is a search for more information on specific issues and this is the whole point in having presentations, where feedback can be generated. To avoid these questions defeats this objective. Where a delegate is seeking confrontation the person may be asked to meet separately to discuss any specific problems.

Ensure that eye contact is made with all in the audience It is more effective to include all in the room by looking at each person from time to time. Larger audiences make this more difficult. It is inexcusable to focus on a few key persons who appear to openly support the presenter.

Move around in a controlled fashion and use the various facilities properly The PowerBeam (or overhead projector) may be used as the main focus of the presentation. The flip chart may be used to set up diagrams and key pointers. The dry ink board may be used in a response to questions by setting out models and matrices to illustrate the answer that is provided. These diagrams will be erased as new ones are drawn so they should not be used for permanent items. Make sure it is possible to move closer to group members as occasional closer contact may be used to control the group. An awkward person can be contained where the presenter moves closer to them.

Speak clearly and always repeat what has been set out on an acetate This not only retains control but also helps those with poor sight or concentration. It is good practice to summarize what has been said at regular intervals.

Negotiate and do not assume a fixed position where reasonable points are raised The auditor should not engage in heated discussion but must rise above the emotions present. Strong arguments can be smothered by simply noting them with no particular response. A ploy is to get another person to respond to sensitive points by asking whether others agree.

Ensure that working papers are available for detailed queries, although we may defer the response if further research is required Give overview answers but defer more detailed ones.

Relax and watch out for nervous gestures which distract Playing with keys or a watch creates an annoying distraction and this can become obsessive behaviour if left unchecked.

Control the audience and move them along when a point has been fully dealt with Most people recognize when one person is overreacting or making too many enquiries and they will not object if the auditor moves them along in a diplomatic fashion. If the structure is put up on the wall then we may tick each one off and suggest we move to the next as each matter is explored.

Audit presentations are about bringing to management's attention the problem, its cause, the effect and required changes This can be done quickly and effectively where the facts are explained and brought to life. We need to refer to matters that affect management and the operational area; this may range from staff cuts or competition to new computers. The idea is to capture the attention of those present in the opening few minutes. We can then go on to explain the control implications and how these may be met by improvements to risk management practices, in line with the adopted recommendations.

Managers are entitled to assume risks where no action is taken, although the implications should be carefully set out As long as they understand the significance of audit recommendations the management takes full responsibility for them. This understanding may be checked during a presentation. The audit position will be to advise and not instruct managers and this must be reflected during the presentation. We need to explain why recommended actions are important.

Professional presentations lift the audit image and get management on audit's side The auditor looks impressive if the presentation is well planned. The CAE must insist on preparation, audit manager input and standards governing the conduct of such meetings.

We may use the opportunity to educate management in both the role of internal audit and the importance of effective risk management and internal control The questions and answers part of the presentation can be used to sell the audit product and pass over ideas to management such as self-audit. We will highlight the importance of the audit report by selling the role of controls as fundamental to the achievement of operational objectives. This educational role should be a theme throughout the presentation.

We may place alternatives in front of management and the resulting feedback may make evaluation and a final decision easier Negotiation skills come to the fore although it is not wise to simply throw away major audit findings as might occur if this is taken to the extreme. Do not ask managers for snap decisions as this is unfair and creates undue pressure. The presentation is to sell the audit report as a serious document worth considering and not to get instant agreement on complicated points.

Questions should be encouraged since a silent audience may indicate that the presentation has not been a success If questions are left unanswered or unasked then management and audit have not fully communicated. A skilful presenter will draw out questions from the audience without allowing one party to monopolize. Detailed questions that require review of the working papers should be deferred rather than hold up the entire presentation and this point should be made at the outset.

Generally the burden of proof falls on internal audit since management will not take action or redirect resources unless for good reason It is part of the audit role to persuade them by constructive reasoning. Change must be justified and cannot occur for its own sake. The presentation raises the profile of the audit and injects life into the report.

An Approach to Audit Clearance Procedures

One approach to audit presentations is to use them in the report drafting procedure to involve management and get an interactive response from them:

1. Complete field work with ongoing discussion with management on findings as they arise.
2. Draft a report that sets out work done, findings and recommendations.
3. Hold a presentation where the report is discussed, concentrating on the outline recommendations as the most important part. Give out the draft report at this meeting and 'sell the ideas'.
4. Ask management to consider the detailed report and meet again for its response. An action plan should then be formulated.
5. Review the report to take on board any matters that management has brought to your attention.
6. Send the report out for wider consultation with all who feature.
7. Prepare final report for formal publication.

There is no point in convening a presentation where the relationship between internal audit and the client is impoverished or has broken down. The presentation then becomes point scoring with little constructive work possible. There is nothing to be gained from a presentation where the underlying audit has not been professionally done. Where findings are flawed, recommendations unworkable and/or the auditor has not been objective, the work cannot be defended in a presentation.

9.10 Audit Committee Reporting

Activity reports are produced periodically by the CAE to formally report the activities of the internal audit department. These would typically go to the audit committee and may be based around an annual report and four separate quarterly reports.

Quarterly Reporting Cycle

The quarterly reports will tend to include:

Planning and control matters for the audit department This will explain whether there are issues and developments that affect the scope and effectiveness of the audit function now and in the near future. This may be seen as a form of self-audit and if an internal or external review of audit has been completed then this will also feature in the quarterly report.

An outline of audit's performance for the quarter This provides results of performance indicators that measure quality and quantity of audit work. These indicators include:

- Level of recoverable work
- Number of reports issued
- Number of audits within budget

Statistics on types of work performed and departments charged This will indicate the work that has been performed over each main department/section. These figures can be compared to planned profiles as a way of gauging the success and viability of the audit function. We would also expect statistical analysis to be carried out over periods as well as between components (e.g. types of work).

Brief summary of reports issued A brief account of the conclusions from final cleared reports may be provided for information. It may be possible to enclose the executive summaries of these reports as appendices to the quarterly audit report. The audit committee may take action where there are matters that remain unresolved arising from audits that have been carried out. However, it should be noted that audit credibility may be damaged where we have 'cried wolf' too often.

Details of staff turnover Information concerning starters, leavers, training programmes and exam success, transfers and any skills gaps should be included since it may have a direct impact on the audit plans. Where additional resources are required to cover audit plans then this should be discussed before a formal bid is submitted via the agreed mechanism.

Overall productivity per output within time budgets This will be based on achieving the quarterly plan, the monthly plan and the requirements of the assignment plan. As such actuals will be set against plan and conclusions drawn about any variances that are so highlighted. Managerial concerns such as budget overruns, excessive unrecoverable time, and incomplete audits will have to be fully explained in the quarterly report, which will act as a high-level control over the audit function.

Many are now seeking to assess internal audit's performance in terms of outcomes rather than outputs. For example, some people feel that an organization should measure the state of its

control environment (through surveys and assessment) and assess the extent to which it is improving. If audit is contributing to a better understanding of internal control, compliance and the management of risks generally throughout the organization then targets may be set and considered in respect of these matters.

Note that the vexed issue of assurance reporting is mentioned in Section 10.11 below.

Annual Reporting Cycle

As well as recording the work carried out over the last year, reference will be made to the annual plan that will also be submitted for the coming year. As auditors, we will be aware that reports can act as key controls so long as they are linked to a reference point in terms of expectations, that is a form of plan. There is a timing problem in that the planning period will start before the report can be available and this gap has to be dealt with through interim measures. The main point is that the report will discuss the control problems of the organization, while the plan will seek to address any continuing disorder. The current audit strategy and how far audit plans, based on this strategy, have been accomplished will therefore be a feature of the report.

The annual report must be received by the highest levels of the organization, ideally a suitably constituted audit committee We have argued that the annual audit report is the final device that ensures that audit's findings are published to the organization. The problem arises where the report falls on deaf ears and is not properly dealt with by the organization. The main safeguard is to ensure that it is received at the highest possible level in the organization as a point of principle.

All comments relating to particular audits should be based on final audit reports, that is, not uncleared drafts that management has not yet been able to respond to There are several dangers if this factor is ignored. It is tempting to get newly drafted reports to the audit committee as a way of boosting the number of reportable items (which will tend to imply an increase in performance of the audit unit). Uncleared reports represent audit views that have not been answered by the people who are responsible for what is being reported. This is a fundamental point of principle designed to be fair for both sides which should be properly observed.

Where the annual reporting period has expired then the current position must be available in outline to members of the audit committee so that the information that is provided is up to date The technical fact that the formal reporting period relates to a date several months old, should not prevent the CAE from providing a current position to the audit committee. This is because it can be frustrating for the organization to dwell on the past when new problems are uppermost on their minds. The rush to get new data just before the relevant audit committee meeting should act as an inspiration to all audit staff, notwithstanding the additional stress that this might create.

Performance data covering internal audit should be based around comparing actual results to planned targets This should be presented in a suitable statistical table that encourages relevant questions from the audit committee. We need to 'come clean' on audit's performance over the year in question. This will not be on a detailed level that is a feature of the quarterly audit report, but must still indicate the general direction of the audit function based around defined expectations. Douglas E. Ziegenfuss has reported on the IIA's Global Audit Information Network's (GAIN) comprehensive research into performance measures, which are summarized below:

Top five performance measures:

1. staff experience
2. auditing viewed by the audit committee
3. management's expectations of internal auditing
4. percentage of audit recommendations implemented
5. auditor education levels

Performance areas ranked by CAEs:

1. auditor quality
2. quality of findings
3. accuracy of reports
4. management satisfaction
5. audit planning
6. standing with audit committee
7. auditee relations
8. organizational status
9. audit committee effectiveness
10. timeliness of reports
11. audit resources
12. quality assurance
13. audit mix
14. compliance with audit plans
15. auditor quality
16. quantity of findings

GAIN Performance Measures – Four audit processes and 16 performance areas: note that each of the 16 performance areas is covered by one or more measures to give a total of 85 separate areas for consideration.

A. Audit environment

1. organizational status
2. audit mix
3. audit planning
4. management satisfaction
5. quality assurance
6. standing with audit committee
7. audit committee effectiveness

B. Input

8. auditor quantity
9. auditor quality
10. audit resources

C. Process

11. auditee relations
12. compliance with audit plans

D. Output

13. quantity of findings
14. quality of findings
15. timeliness of report
16. accuracy of reports[23]

A view on the overall state of risk management and internal controls (possibly over the main key control areas) should be expressed along with the main implications of any material weaknesses and how these might then be tackled. We have an opportunity to paint a blanket picture of the control environment that can be understood by top management. This should be in the form of general assurances in a suitable paragraph that has been carefully highlighted in the report. It should fall in line with the auditors' professional obligation to deliver a formal opinion derived from the detailed work undertaken within the organization. Nothing short of this will suffice. The IIA has defined adequate control as being present if:

> Management has planned and organized (designed) in a manner that provides reasonable assurance that the organization's risks have been managed effectively and that the organization's goals and objectives will be achieved efficiently and economically.

A suitable format for the annual report should be decided beforehand It is as well not to complicate issues by including an abundance of detail that will make the report unnecessarily long and possibly unreadable. The needs and demands of the audience should be firmly kept in mind when deciding the adopted approach. We must also consider the marketing angle where a hint of professional presentation will always be well received by the committees.

The annual report will be formed more at an overview level Some very poor reports appear to make global statements derived from basic management theory while quoting a stream of minor matters that have very little significance to senior management at all. Missing invoices are mentioned in the same sentence as major conclusions about controls generally in the organization, which is a big mistake. We are only entitled to comment on important matters where work has been done at the same level or we risk an impaired credibility. Hopefully, we will have completed major reviews during the year to enable a sensible conclusion to be reported. If this is not the case we must go back to basic principles, and ask why this is not happening. Mary Combs has explained how an assurance framework can be used to drive the annual audit opinion:

> The assurance framework is designed to provide definitive assurance to the board, the CEO and other layers of management that the organization is credible, can be relied upon to deliver on its objectives and to manage its risks and that stakeholders can be confident it will do so. The assurance framework is accomplished using nine primary tools. These are:
>
> 1. Risk reviews of management of specific significant risks;
> 2. Risk process reviews of the risk identification, assessment and reporting processes;
> 3. Control reviews looking at processes, critical systems and compliance with laws and regulations;
> 4. Review of the organization against its model control framework;
> 5. Value assurance reviews on major projects;
> 6. Policy evaluation programme looking at longer range impacts of policy decisions;
> 7. Statistics for progress on audit findings and
> 8. Risk action plans;
> 9. Letters of assurance.
>
> The results are used as the basis of the annual audit opinion, which is one of the key supporting documents to enable the board and the executive chairman to sign the Statement of Internal Control and other disclosure documents with confidence. The risk and assurance programme, which has been in use since vesting, gives assurance that the system of internal control is operating effectively.[24]

Problem areas encountered over the year This may be in terms of access to information, formulating audit plans and keeping up with developments within the organization. We may have to use the powers of the audit committee to provide what in the final analysis will be a complaint that is brought to the attention of the organization. Problems securing information (e.g. downloads of sensitive databases such as personnel) should be brought before the audit committee as a way of stimulating discussions on resolving these concerns. Specific matters will have been dealt with at an earlier stage as problems arise. General problems such as a tendency for managers to fail to implement audit recommendations must also be exposed, if there has been no success resolving this difficulty beforehand. We would obviously use this technique carefully but it can be a powerful aid to the auditor where all else fails.

Pensive thoughts on the current state of the audit function and barriers to good performance All foreseeable barriers should be broken down by setting out ways that they may be dealt with. We would conclude with a look forward to the coming year in terms of the problems that the organization faces and how the proposed audit strategy will take on board and deal with relevant control issues.

These reports may well help determine the level of support that audit receives and whether the internal audit function survives in times of budgetary constraint. They also remove the mystique behind audit and make it quite clear that, like all other functions, internal audit is also accountable for its resources and actions.

9.11 New Developments

We start this section on new developments by looking at the problems thrown up by corporate fraud. The scale and scope of fraud is captured by Arthur Piper in a special report on the rise of fraud in the UK:

> After years of uncoordinated attempts by legislators, regulators and the police to get to grips with fraudsters, the authorities seem to have suddenly woken up to the reality that tacking fraud should be a national priority: not least because fraud is big business. It costs the UK and estimated £14bn a year, which is over £230 per person in the country. In fact, fraud is on the increase because of the economic downturn. The business services firm, the Network, has recently found that the number of fraud-related reports surged from 10.9% to 21% from the first quarter of 2006 to the first quarter of 2009, in its 2009 Benchmarking Report. The report also confirmed that in-house fraud is on the rise.[25]

Internal auditors are expected to deal with fraud and when discussing current developments, the so-called expectation gap will not go away. That is, there is often an assumption that internal audit is responsible for managing the risk of fraud. Neil Baker has outlined relevant guidance from the IIA:

- Investigating the causes of fraud
- Reviewing fraud prevention controls and detection processes put in place by management
- Making recommendations to improve those processes
- Advising the audit committee on what, if any, legal advice should be sought if a criminal investigation is to proceed
- Bringing in any specialist knowledge and skills to assist in fraud investigations, or leading investigations where appropriate and requested by management

- Liaising with the investigation team
- Responding to whistleblowers
- Considering fraud risk in every audit
- Having sufficient knowledge to identify the indicators of fraud
- Facilitating corporate learning[26]

Some fraud investigations use surveillance to obtain evidence that cannot be gathered in any other way. In the past, this was fairly straightforward. In more recent times, the internal auditor has had to adhere to rules on using this approach as governments tighten up what may be seen as an infringement of human rights. The UK's Information Commissioner's Office views surveillance are the purposeful, routine, systematic and focused attention paid to personal details, for the sake of control, entitlement, management, influence or protection. Controls that track or monitor an employee's actions and communications have to be used with care so as not to be an abuse of power. Most agree that organizations need a strategic approach to fraud if they are to stay on top one step ahead of the international fraudsters that are fast becoming the corporate risk. The Chartered Institute of Public Finance and Accountancy has a simple checklist on this matter:

1. Does the organisation have a counter fraud and corruption strategy that can be clearly linked to the organisation's overall strategic objectives?
2. Is there a clear remit to reduce losses to fraud and corruption to an absolute minimum covering all areas of fraud and corruption affecting the organisation?
3. Are there effective links between 'policy' work (to develop an anti-fraud and corruption and 'zero tolerance' culture, create a strong deterrent effect and prevent fraud and corruption by designing and redesigning policies and systems) and 'operational' work (to detect and investigate fraud and corruption and seek to apply sanctions and recover losses where it is found)?
4. Is the full range of integrated action being taken forward or does the organisation 'pick and choose'?
5. Does the organisation focus on outcomes (i.e. reduced losses) and not just activity (i.e. the number of investigations, prosecutions, etc.)?
6. Has the strategy been directly agreed by those with political and executive authority for the organisation?[27]

IT governance is the next big ticket item that is starting to appear on the boardroom agenda as businesses are increasingly relying on e-business solutions. The IT auditor has an eye on IT risks and how they are being managed across the organization. In more recent years, there has emerged a new and improved chief information officer (CIO) who has much the same views, and is quite happy to listen to the auditor's views on risk management that focuses on information systems. The CIO's position is made clear in the following extract:

> Risk is an inherent part of doing business, and in a dynamic and global marketplace where change and uncertainty are the norm, risk rises exponentially. Corporate acquisitions, collaborative partnerships, global integration and accelerating technological advances all create risk, and today's most successful businesses have learned to absorb and mitigate it with relative ease. These companies are not only weathering change, they are taking advantage of it and, in some cases, even instigating it to uncover new opportunities. Such resilience is key to long-term growth and profitability. With virtually every aspect of modern business linked to information technology (IT), resilience increasingly depends on a company's ability to effectively manage the risks introduced into its IT and physical infrastructure and processes. It's no wonder that for today's top CIOs, risk management is not just a dominant theme; it has become a vocation – just

> as it is for their business line colleagues. Still, the scope of many CIOs' risk management efforts is often too limited to gain real value for the business. The fact is, IT executives are more likely to practice risk avoidance than risk management. And when they focus too strictly on the risks to IT and overlook the risks and benefits to the business, they limit the opportunity to drive financial and operational advantage. Good risk management in today's highly interconnected, dependency-driven business environment requires IT leaders to see and understand the business investment and financial upside of risk-taking. A holistic and more broad-based view of risk enables them to recognize the impact that IT processes and the infrastructure can have on business activities. They are better equipped to leverage IT's ability to reduce risks to the business and capitalize on opportunities for profit. A risk-aware governance framework facilitates this broader business perspective by providing decision makers across the organization with a more complete picture of risk and the potential for return. They gain the panoramic insight to make decisions that maximize revenue potential while levying an acceptable level of risk. They are better able to implement effective analysis and automation to address current risks while protecting the emerging interests of the enterprise. In short, they can achieve a better balance of risk and return. CIOs who can communicate the business importance of risk management for IT and the related physical infrastructure can transform the way the IT leaders – and the entire enterprise – approach risk. More importantly, they can turn traditional IT risk management into a compelling, value-generating opportunity for the business.[28]

Building on the way the auditor can work with the chief information officer to raise the profile of IT as a boardroom agenda item, we can turn to a further view on this topic:

> As IT represents only a part of the overall board agenda it is vital that NEDs have the right tools and information with which to challenge IT constructively and effectively ask the right questions. Coupled with the above, internal audit needs to position itself as the independent navigator of IT assurance. Given that the board will be receiving differing levels of assurance from, amongst others, compliance, IT security, third parties, project steering committees and the chief information officer (CIO), internal audit could integrate and quality assure this assurance, acting as an effective translator and trusted adviser. Chances are that existing assurance providers will be communicating risk inconsistently, providing an incomplete view of IT governance. What the board needs is effective translation of the business message embedded in technical jargon – and this is a role that an independent internal auditor is ideally placed to fulfil.[29]

Sticking to the high view of IT, one interesting development is work carried out by members of the INFOSEC Research Council (IRC), who are the major sponsors of information security research within the U.S. Government. Taking a high-level strategic view of IT security issues, they have been developing a hard problem list that over the next five to ten years covers the following areas:

1. **Global-Scale Identity Management:** Global-scale identification, authentication, access control, authorization, and management of identities and identity information.
2. **Insider Threat:** Mitigation of insider threats in cyber space to an extent comparable to that of mitigation in physical space.
3. **Availability of Time-Critical Systems:** Guaranteed availability of information and information services, even in resource-limited, geospatially distributed, on demand (ad hoc) environments
4. **Building Scalable Secure Systems:** Design, construction, verification, and validation of system components and systems ranging from crucial embedded devices to systems composing millions of lines of code.

5. **Situational Understanding and Attack Attribution:** Reliable understanding of the status of information systems, including information concerning possible attacks, who or what is responsible for the attack, the extent of the attack, and recommended responses.
6. **Information Provenance:** Ability to track the pedigree of information in very large systems that process petabytes of information.
7. **Security with Privacy**: Technical means for improving information security without sacrificing privacy.
8. **Enterprise-Level Security Metrics:** Ability to effectively measure the security of large systems with hundreds to millions of users.

These eight problems were selected as the hardest and most critical challenges that must be addressed by the INFOSEC research community if trustworthy systems envisioned by the U.S. Government are to be built.[30]

One high-level approach to IT auditing is to consider the data security guidelines that are used in the organization and this approach has been described as follows:

> A widely recognised auditing standard developed by the American Institute of Certified Public Accounts. An independent audit of an objective's "control objectives and control activities", it normally includes checks on controls on information technology and related processes. An independent accounting or audit firm will do the audit and publish two types of report. A "type one" report, describes the organisation's controls at a specific point in time. A "type two" report describes an organisation's controls over a minimum period of six months. Information Security Management is the only auditable international standard for information security management systems. The British Standards Institute says that being certified to ISO 27001 will help organisations manage and protect information assets. The standard is designed to ensure the selection of "adequate and proportionate security controls". It is based around monitoring, reviewing and improving information security management systems. The standard is applicable for all sizes of organisation and is particularly suitable where the protection of information is critical, such as in the finance, health, public and IT sectors. The standard is also used by outsourcing suppliers to assure customers that their information is being protected. ISO 27001 comprises a checklist of 133 information security controls which an organisation should consider. These controls include data backup, controlling access to a computer network, passwords, and encryption. The standard is not prescriptive; organisations must prove that their information security controls are adequate for their organisation. The certification process is usually in three stages. Stage one is a review of the existence and completeness of key documentation such as the organisation's security policy, "statement of applicability" and "risk treatment plan". Stage two is an in-depth audit involving testing the existence and effectiveness of the information security controls stated in the SoA and RTP, as well as their supporting documentation. The final stage is an annual audit to confirm that a previously-certified organisation remains in compliance with the standard. The cost of certification is about £900 per day. Getting the certification can take a couple of days to a couple of months, depending on the size of the organisation.[31]

Our final emerging topic is the growing importance of corporate assurance maps. Closely related to positioning the audit function to add value to the business is high impact auditing that derives from a strategic focus on the corporate risk management process. It is a good idea to get straight to the point when performing field work. Gone are the ways of working through a detailed checklist of tests that are applied to the audit as a standard routine. There are still many audit checklists in existence but their use is being questioned as we move to an objective-based approach. Audit fieldwork can be about five basic elements:

1. Being clear about the operational objectives in the area being audited and how these objectives create and preserve value for the business.
2. Understanding the business model in place and the way risk is dealt with through the adopted business strategy and effective leadership in delivering the strategy through performance review and meaningful incentives.
3. Working out how the risk managed process ensures that these controls work to retain risk within an acceptable risk appetite that the process owner is then accountable for.
4. Considering how the manager obtains an oversight of the way the operation is governed, compliance is ensured and how assurances along with significant risks are reported upwards.
5. Reviewing the risk management reports for consistency, reliability and whether the reports themselves enable management to make good decisions and account for their responsibilities.

The auditor may want to take a view on each of these elements although it is the final point, five, that is most interesting. The auditor should encourage business managers to be a firm part of the assurance-giving process along with the other assurance teams that work in the organization. But what do we do when the business has not got a handle on risk management that is, risk immature:

> Let us consider risk immaturity. All organisations are risk immature to some degree. Managers across many sectors fail to set clear objectives, identify risks that flow from those objectives and adequately mitigate those risks. Looking at recent corporate failures, including an entire business sector, can we really argue that risk maturity is prevalent, or even dominant? As the private sector suffers from an economic recession, it is clear that many management teams have failed to take risk management seriously, or have struggled to apply it effectively. The public sector, as it shortly enters its recession, is likely to be similar . . . .These circumstances mean that internal audit must have a new paradigm and professional culture that recognises risk immaturity. Internal audit needs to adjust to the reality of a risk immature world. This is not to say that risk immaturity is acceptable or desirable, more to recognise that it is more prevalent than currently publicly acknowledged or accepted . . . .I think, therefore, it is time for the profession to recognise the risk immaturity of many organisations and their management teams. Now is the opportunity, with such a widespread recognition of risk management failure in so many organisations, for internal auditors to lead in the identification of nominal or poor risk management. Internal audit should be brave enough to report where risks are not being assessed and managed properly rather than being complicit in the box-ticking risk management exercise undertaken in some organisations. Internal auditors should be recognised as the risk management professionals that they are.[32]

The auditor needs to work out how well the business is doing in managing risk and providing an account of this task. During the audit, it is possible to consider the way assurances are being provided on controls and whether there is an integrated approach to this task. Health and safety, legal compliance, IT security and other teams may each have had an input to opining on controls in various business units. Some of the risks that are considered during the audit may have been reviewed by other assurance teams and it may be possible to view the results as part of the audit fieldwork process. This approach is organic and is far removed from the old approach of working through a checklist of audit tests to complete the fieldwork. Some auditors argue that they use checklists to make sure they have covered all key areas or have completed all important tasks. Others develop their own checklist as they progress through the audit fieldwork rather than use an off-the-shelf version. Still others refuse to use any form of checklist at all. At the end of the audit fieldwork, the audit may be able to report on whether:

1. Operational objectives are clear and they create and preserve value for the business.

2. The business model and the adopted business strategy are delivering these objectives through effective leadership and meaningful performance incentives.
3. Controls work to retain risk within an acceptable risk appetite.
4. The manager is able to govern the operation and provide assurances that significant risks are addressed and where appropriate, reported upwards.
5. Risk management reports are consistent, reliable and lead to good decision making.

This is far removed from audit reports that simply reproduce detailed lists of minor errors in specific processes that need to be put right by management. The auditor is really looking for the assurance map that reflects the oversight responsibilities across the organization. This map is either present or which needs to be developed to show:

- the types of assurances required by the board;
- who gives these assurances and in what format;
- how these assurances are verified to ensure they are entirely reliable and kept up to date;
- how can executives be assured that reckless behaviour is not happening in the organization.

This last point is significant. How can the board know if people they employ are exceeding the risk appetite, that is, they are being reckless with corporate resources. Senior Supervisors Group, of banking representatives from Canada, France, Germany, Japan, Switzerland, the UK and the US, have commented that:

> A key weakness in governance stemmed from what several senior managers admitted was a disparity between the risks that their firms took and those that their boards of directors perceived the firms to be taking. In addition, supervisors saw insufficient evidence of active board involvement in setting the risk appetite for firms in a way that recognizes the implications of that risk taking. Specifically, only rarely did supervisors see firms share with their boards and senior management a) robust measures of risk exposures (and related limits), b) the level of capital that the firm would need to maintain after sustaining a loss of the magnitude of the risk measure, and c) the actions that management could take to restore capital after sustaining such a loss. Supervisors believe that active board involvement in determining the risk tolerance of the firm is critical to ensuring that discipline is sustained in the face of future market pressures for excessive risk taking.[33]

In terms of understanding exactly what reckless behaviour might look like, we need go no further than the words of Chuck Prince, in July 2007, the ex CEO of Citigroup, who said about the now infamous Credit Crunch:

> 'When the music stops, in terms of liquidity, things will get complicated. But as long as the music is playing, you've got to get up and dance.'

Extreme reckless behaviour should stand out in any well-run organization by being exposed on the board level assurance map and when reviewing the assurance map, Southampton City Council auditors try to make sense of assurance routines as explained by their chief internal auditor:

> Sarah Dennis, chief internal auditor at Southampton City Council, says that getting management agreement could be extremely time-consuming, but was an essential part of producing a good report. She advises internal auditors to focus on the top five messages it wants to get across. Her favourite question to any issue raised by her team is, "so what?" Each point needs to link business

> objectives to key risks and the audit observations and actions need to be clearly relevant to those objectives and risks. While Dennis issues a clear opinion, coded red, amber and green, she does not make recommendations, but lists agreed management actions. Jonathan Lovering, head of audit at Henderson Group, sees the role of his function as providing combined assurance to the audit committee and executive management. "With increasing corporate governance, the audit committee is receiving all sorts of compliance and assurance from the business," He explains. "Internal audit decided to say how its work dovetails with those assurance sources and to give a combined overview of assurance on top of what each of those functions is doing."[34]

With the increasing reliance on assurances, it is clear that they must be reliable and give value to the business. Essentially, assurances give confidence to the recipient that all is well, or that current action is in hand or that something new needs to be done. It is implicit in the assurance that the provider of these assurances is professional, independent and has carried out sufficient examinations to be able to hold an opinion. And there is documentation that supports the assurances and the process from which they were developed. The big question then is, can the summation of individual audits enable the CAE to provide assurances that comment on the entire organization? Or should the CAE start to prepare corporate wide reviews of the assurance infrastructure and implant audit work within these maps to give a holistic picture of the quality of risk management within the organization. One way of getting to grips with the assurance map is to take the various committee that report into the main board and argue that these bodies represent the assurance infrastructure in that each committee is there to give assurances on a major aspect of the corporate issues that are uppermost in the minds of the board. Internal audit may be moving to a position where they will be reviewing the extent to which these committees work in giving assurances on areas that they are charged to take care of. Although internal audit can never set the level of acceptable risk, it can comment on the extent to which risk managed is aligned to what is viewed as acceptable by the board. It may be the case that the internal auditor will need to select a position from one of four points:

1. Being part of the corporate assurance map by giving assurances in defined parts of the business.
2. Coordinating the assurance map by ensuring all assurance teams work together and fit into the enterprise-wide risk management process.
3. Reviewing the assurance-giving process to ensure it makes the best use of available resources and gives the board the service it requires.
4. Leading the assurance process that seeks to review and help improve the enterprise risk management process.

Summary and Conclusions

This chapter has provided an introduction to audit field work, from planning through to performing and reporting the engagement. Note that IIA practice advisory 2210.A1 suggests that internal auditors consider management's assessment of risks relevant to the activity under review. The internal auditor also considers:

- the reliability of management's assessment of risk;
- management's process for monitoring, reporting and resolving risk and control issues;
- management's reporting of events that exceeded the limits of the organization's risk appetite and management's response to those reports;
- risks in related activities relevant to the activity under review.

The need to build the state of risk management into the audit approach calls for some flexibility in the way audits are undertaken. We have mentioned interviewing, and the wider task of ascertaining the system, evaluation, testing techniques and communicating the results. In one sense, we have tried to write about something that is impossible to capture in one idea, that is the combination of risk-based systems audits, reviews, investigations, consulting projects and short exercises that typifies the internal auditors' work. Moreover, there really is no such thing as audit field work. There are only different types and approaches to audit work that suit different contexts and challenges. One possible approach (developed by the author), albeit fairly general, is to frame the audit work around a model that we have called ICE, internal control evaluation. It is better referred to as risk and control evaluation (RaCE) and, as a model, can be applied to many different approaches to audit assurance and consulting services. Our RaCE model appears in Figure 9.31.

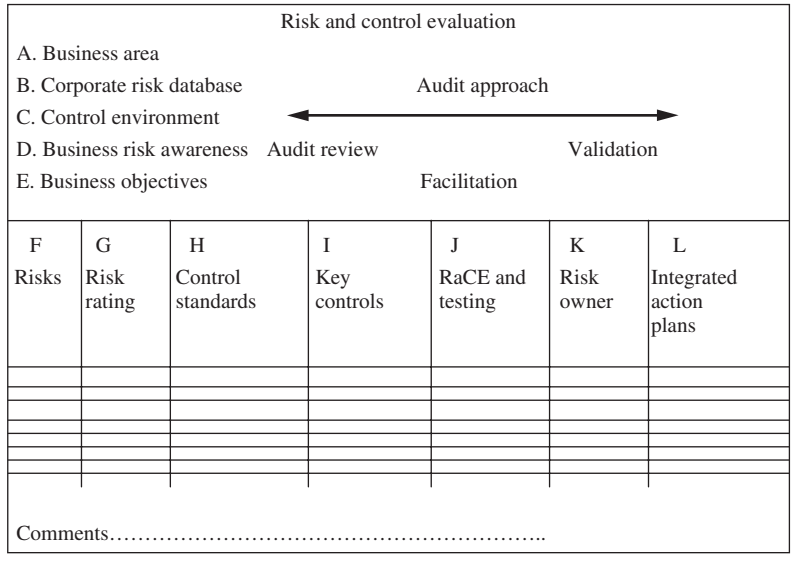


FIGURE 9.31 The RaCE approach.

The model is an interpretation of an audit approach that does not start with the need to 'catch people out'. It is based on adapting the approach to the context in question, and moving between the extremes of *audit review, facilitating* the client's assessment to simply *validating* the current self-assessment process. A useful quote on the concept of audit findings comes from Larry D. Hubbard who wrote:

> The term 'finding' is actually a misnomer. If a problem exists, auditors are not usually the ones who discover or identify it. Instead, it's more likely that the workers or management in the area already knew of the problem but just haven't addressed it yet. Calling this a finding suggests that our clients were hiding the problem and that we found it – a 'hide and seek' game between auditors and clients that organizations don't need to play. I prefer to label the issues encountered during an audit as either 'ineffective controls' or 'risks that have not been addressed' . . . A good audit report entails positive news for our clients. Or, as management might say, 'the best audit report is no audit report at all'.[35]

Using the alpha references A to L, the RaCE is explained in outline:

A: First identify exactly what business area is in the annual audit plan. This may be a section, team, project, process, change programme, local office, establishment, contract, business unit or whatever is deemed to be a distinct auditable area.

B: The next step is to find out where the business area (BA) stands on the corporate risks database in terms of relative risk in the organization. This should have been done to form the basis of the annual audit plan.

C: It may then be possible to assess the control environment in the BA. COSO and CoCo each have assessment questions and guidance that can be used to judge whether the BA is on a sound footing in terms of having an environment that reflects the corporate position in a trustworthy and reliable manner.

D: The next stage is to assess the extent to which risk and control assessment is understood and practised in the BA. Where there is a developed risk assessment procedure and good appreciation by managers, supervisors and staff generally, then we can start to judge where the BA stands in terms of having a robust risk management process in place and reliable risk registers.

E: This is simply isolating the agreed business objective of the BA in question.

Armed with the knowledge secured from the assessments A to E above, the audit approach may be determined. This may entail performing a standard audit (Audit review) where the control environment and level of risk appreciation is such that it is not possible to rely on a facilitated self-assessment review. Where the BA has a good control environment but is not equipped to carry out the risk assessment, then a facilitated (Facilitation) approach may be provided by the audit team to help the client get up to par. Where both the control environment promotes integrity, compliance and competence and self-assessment is being applied then audit may simply validate (Validation) the self-assessment already used by the BA, and concentrate on key controls that have been deemed important in managing the more material risks.

F: Risk to the achievement of business objectives are defined and updated to reflect current changes. For well-performing BAs the risk assessment will be based more on the future strategy, since the current position is already successfully managed.

G: Risk rating is simply the degree of materiality and likelihood that forms the basis for most risk assessment models.

H: Control standards are mechanisms that may be applied to managing the business risks that have been isolated in G.

The tasks F to H may be performed by the auditor (for the Audit approach), a convened workshop of client staff facilitated by the auditor (Facilitated approach) or through an examination of the current risk assessment already carried out by the client management (Validation audit approach).

I: This involves identifying the key controls in use.

J: The evaluation stage comes next where the key controls are considered in terms of whether they are sufficient to manage the risks, as compared to the control standards developed in H. Testing is carried out using the audit approach, while audit effort will focus on judging whether the client is able to assess compliance under the current arrangements. Where the RaCE is found to be sound on a self-assessed basis then the auditor may focus on validation and may perform some limited independent testing to check that controls are working properly.

K: Each risk assessment should be assigned to a risk (or process) owner so that it is clear where responsibility and accountability lie.

L: This part of the RaCE simply states that action required to manage risks is integrated within the current performance management arrangements. The way this is done is entirely up to the manager so long as the risks in question are dealt with in an efficient and effective manner in line with the corporate risk policy and defined risk appetite.

Where the auditor captures the above information in the RaCE, this process can drive the audit so that ascertainment is about identifying the system and risk (e.g. the flowchart and interview record), evaluation features in column J cross-referenced to the auditors' records and testing schedules are referenced to the lines in column J. Audit recommendations are based around findings from the evaluation and test results and feature in the final column L. The audit report is then a representation of the RaCE and describes the system, the risks, how they are managed and anything more that needs to be done to help ensure business objectives can be achieved. Where the RaCE has been performed by the client staff and facilitated by the auditor it becomes a joint effort between audit and client with some formal testing performed by the auditor. Where the RaCE has already been recently performed by the client, the auditor validates the work, updates the RaCE, performs selective testing and then is able to provide assurances on the adequacy of risk management and the underlying systems of internal control. The RaCE process depends on all parts of the organization embracing the risk management concept and using internal audit to assist this task with a mixture of assurance and consulting input depending on which approach best suits the business area in question. In this way the auditor:

- recognizes that some business areas can be relied on to self-assess their systems and audit only needs to validate (and check) the arrangements in place;
- helps those business areas that need to develop their risk assessment practices and so assesses their progress at the same time;
- reviews areas where there are obvious problems and makes recommendations to improve the control environment and get risk management practices put in place. Audit will be concerned that the integrity and competence of people within the business area is properly developed.

In this way, audit field work may then be performed in a way that is both flexible and dynamic and makes sense to the client manager, board and the audit committee.

Chapter 9: Assignment Questions

Having worked through the chapter the following questions may be attempted (see Appendix A). Note that the question number relates to the section of the chapter that contains the relevant material.

1. Describe how the preliminary survey may be used to arrive at the terms of reference for an audit and discuss the different interpretations of the role of audit programmes.
2. Describe the importance of effective interviewing for the internal auditor and discuss the ways in which the auditor can ensure that such interviews have a good chance of success.
3. Explain the different ways that a system may be ascertained and recorded and describe the factors that should be considered in deciding whether a system's flowchart should be prepared.
4. Consider and illustrate by the use of brief examples the two techniques of ICQ and ICES and describe their respective merits and disadvantages.
5. Explain the importance of audit testing and discuss all those issues that need to be considered when deciding on the types and depth of tests that are applied.
6. Explain the attributes of good audit evidence and describe the sources that may be used to gather suitable evidence to support the audit opinion and report.
7. Explain the concept of statistical sampling and consider the ways this technique may be applied to provide an enhanced audit product.
8. Describe the different types of reports that may be prepared by the internal auditor and discuss the factors that make for a well-received and effective audit report.
9. Describe the measures that can be taken by an internal auditor to help ensure the formal presentation of an audit report to a senior management team is successful.
10. Prepare a presentation to the internal audit management team covering the information that should be reported to the audit committee in the annual internal audit report.

Chapter 9: Multi-choice Questions

9.1 Which statement is most appropriate?

a. One basic approach that has been discussed is risk-based systems auditing. This involves establishing the system objectives, finding out what risks should be addressed and then developing appropriate solutions to minimize all risks.

b. One basic approach that has been discussed is risk-based systems auditing. This involves establishing the system controls, finding out what risks should be addressed and then developing appropriate solutions to mitigate unacceptable levels of risk.

c. One basic approach that has been discussed is control-based systems auditing. This involves establishing the system objectives, finding out what risks should be addressed and then developing appropriate solutions to mitigate unacceptable levels of risk.

d. One basic approach that has been discussed is risk-based systems auditing. This involves establishing the system objectives, finding out what risks should be addressed and then developing appropriate solutions to mitigate unacceptable levels of risk.

9.2 Insert the missing words:

The preliminary survey seeks to accumulate relevant information regarding the operation under review so that a defined direction of the ensuing audit (if it goes ahead) may be agreed. The ..... will be the first point of call.

a. internal audit files
b. client in question
c. Internet search
d. external auditor

9.3 Insert the missing words:
A feel for the audit can be gathered from impressions gained from ....., where the initial impression can be used to help direct the auditor towards particular problems.
a. thinking about the risks involved
b. touring the work area
c. preparing an outline audit report
d. testing the system

9.4 Which statement is most appropriate?
a. The system selected by the auditor has to be tested before it can be audited and the preliminary survey comes to the rescue. Systems boundaries can only be determined after the necessary information has been accumulated and digested. This must happen before the assignment planning stage so that a clear plan may be documented and shown to management. The aim of the preliminary survey will be to agree the objectives and scope and timing of the audit with management. What needs to be done, how and when.
b. The system selected by the auditor has to be defined before it can be audited and the preliminary survey comes to the rescue. Systems boundaries can only be determined after the necessary information has been accumulated and digested. This must happen after the assignment planning stage so that a clear plan may be documented and shown to management. The aim of the preliminary survey will be to agree the objectives and scope and timing of the audit with management. What needs to be done, how and when.
c. The system selected by the auditor has to be defined before it can be audited and the preliminary survey comes to the rescue. Systems boundaries can only be determined after the necessary information has been accumulated and digested. This must happen before the assignment planning stage so that a clear plan may be documented and shown to management. The aim of the preliminary survey will be to define the objectives and scope and timing of the audit and then inform the management. What needs to be done, how and when.
d. The system selected by the auditor has to be defined before it can be audited and the preliminary survey comes to the rescue. Systems boundaries can only be determined after the necessary information has been accumulated and digested. This must happen before the assignment planning stage so that a clear plan may be documented and shown to management. The aim of the preliminary survey will be to agree the objectives and scope and timing of the audit with management. What needs to be done, how and when.

9.5 Which statement is most appropriate?
a. Systems audits emphasize transactions testing, and the audit programme is formulated at the preliminary survey stage. For compliance and probity audits this detailed testing programme can only be defined after the system has been documented and assessed. The programme of work that is set for a systems audit can be described as an audit guide that determines the work required to complete the audit and this may be drafted at preliminary stage. The programme will include target dates and perhaps a progress checklist for stages of the audit.
b. Compliance and probity audits emphasize transactions testing, and the audit programme is formulated at the preliminary survey stage. For systems audit, this detailed testing programme can only be defined after the system has been documented and assessed. The programme of work that is set for a systems audit can be described as an audit

guide that determines the work required to complete the audit and this may be drafted after the testing stage. The programme will include target dates and perhaps a progress checklist for stages of the audit.

c. Compliance and probity audits emphasize transactions testing, and the audit programme is formulated at the preliminary survey stage. For systems audit this detailed testing programme can only be defined after the system has been documented and assessed. The programme of work that is set for a systems audit can be described as an audit guide that determines the work required to complete the audit and this may be drafted at preliminary stage. The programme will include target dates and perhaps a progress checklist for stages of the audit.

d. Compliance and probity audits emphasize transactions testing, and the audit programme is formulated at the preliminary survey stage. For systems audit this detailed testing programme can only be defined before the system has been documented and assessed. The programme of work that is set for a systems audit can be described as an audit guide that determines the work required to complete the audit and this may be drafted at preliminary stage. The programme will include target dates and perhaps a progress checklist for stages of the audit.

9.6 Which statement is least appropriate?

The Preliminary Survey Report of one or two pages will cover the following:

a. An outline of the system under review including systems objectives and boundaries.
b. The work undertaken on detailed compliance testing.
c. An initial opinion on the risk areas based on the key control objectives covering compliance, information systems, safeguarding assets and VFM.
d. Recommendations for the proposed assignment in terms of the nature and extent of audit cover now required.
e. An appendix with outline systems notes and a draft audit guide/programme for the full audit.

9.7 Which statement is least appropriate?

Factors to be addressed in the assignment plan are:

a. The terms of reference for the audit by audit management and disclosed to the client management.
b. The scope of work including areas for coverage and parts of the system not to be dealt with at this time.
c. Target dates for start and completion and key stages.
d. A full definition of the system under review including the points where it starts and finishes and interfaces with other related systems.
e. Identification of risk areas and critical points of the audit that may require special attention and/or resources.
f. Definition of the reporting and review arrangements including a list of the officers who will not receive draft reports.
g. Establish a confirmed audit programme (or guide) for each part of the audit and the testing regimes (for compliance reviews).
h. The assignment plan will outline any travel and hotel arrangements along with subsistence allowances.
i. Identify the auditors assigned to the project and their roles.

9.8 Insert the missing words:

One solution is to disallow budget extensions unless there is good reason such as to avoid the psychological dilemma of ' . . . . . '. This occurs when the auditors

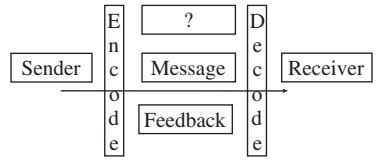
become so engrossed in an operation that they see themselves as an expert who have a duty to solve all problems after mastering the system.

a. extended testing
b. auditor attachment
c. emotional involvement
d. operational engrossment

9.9 Insert the missing word (? In the Figure):

Interviewing is based around effective communications and it is a good idea to remember the basic communications model to appreciate where things could go wrong and how communicating may be improved using the following:

Communications



a. confirmation
b. clarification
c. noise
d. review

9.10 Select the most appropriate percentage (a, b, or c) for the three sources of first impressions (1, 2 and 3):

This initial contact with management is quite important, since some estimate that around 90% of people will decide what they think and feel about someone within the first 10 - 40 seconds of meeting them based on:

Sources of first impressions	**Importance on forming an impression**
1. visual impact (what is seen)	%
2. auditory impact (what is heard)	%
3. content (what is said)	%

Importance:

a. 38%
b. 55%
c. 07%

9.11 Which statement is most appropriate?

a. Post-audit – These potentially difficult interviews bring the main findings to the client's attention once the field work has been completed. If the client has been kept informed throughout the course of the audit then one may avoid confrontational closure meetings. Our reporting standards generally mean that we should not present management with surprises in the formal audit report.
b. Post-audit – These potentially difficult interviews bring the main findings to the client's attention once the field work has been completed. If the client has been kept informed throughout the course of the audit then one may avoid confrontational closure meetings. Our reporting standards generally mean that we should not present management with old news in the formal audit report.
c. Post-audit – These potentially difficult interviews bring the main findings to the client's attention once the field work has been completed. If the client has not been interrupted throughout the course of the audit then one may avoid confrontational closure meetings.

Our reporting standards generally mean that we should not present management with surprises in the formal audit report.

d. Post-audit – These potentially difficult interviews bring the main findings to the client's attention once the field work has been started. If the client has been kept informed throughout the course of the audit then one may avoid confrontational closure meetings. Our reporting standards generally mean that we should not present management with surprises in the formal audit report.

9.12 Which statement is least appropriate?

It is generally advisable to structure the interview since this tends to assist the task of exchanging information. The process should involve the following key steps:

a. Background preparation on the subject area. Whatever the interview it is always useful to do some background work related to the particular topic at hand.
b. Set convenient dates and times. On the basis that an interview that is hurried with the constant pressure of other competing demands lowers the benefits that come from such a forum, it should be arranged properly.
c. Prepare checklist areas to cover. This should entail a brief note of the areas that need to be covered as an aid memoir and as a way of thinking through the information-gathering process beforehand.
d. Define objectives of the interview. The next important stage is to state the precise objectives of the meeting.
e. Set the tone of the interview that should normally be open, friendly and positive. The opening comments are commonly known as 'breaking the ice' and involve focusing on neutral topics such as the competence of management, poor performance issues or potential employee fraud areas, so as to develop some form of immediate rapport.
f. Invite feedback on the audit objective and explain how the interview fits into the audit process. It is one thing to state the audit objective and then break the ice with some opening remarks that show the human face of the auditor.
g. Ask the questions and direct the interviewee to the key issues without restricting the responses. The real hard work comes in the main part of the interview.
h. Run through matters dealt with during interview and clear up uncertainty. It is frustrating to review interview records and pick out points that are unclear or ambiguous.
i. Conclude the interview with the usual courtesies. We must retain a level of diplomacy at all times.
j. Ask for any questions. There must be a clear stage at the end of the interview where the other party is allowed to reflect on what has been said and ask general questions.
k. Explain the next steps. The last consideration is to explain clearly what will happen from here on.

9.13 Insert the missing words:

The auditor poses a threat in terms of the potential for ..... to the working lives of everyone they meet.

a. enforcing procedures
b. promoting changes
c. causing problems
d. mitigating risk

9.14 Which statement is most appropriate?

a. Even where the auditor is involved in investigations into irregularity, there is still a view that the auditor is primarily examining the circumstances at issue and not the people concerned. Where a name can be fitted to a problem, then this should be a natural

consequence of the proceedings and not a witch-hunt. One of the easiest aspects of the audit role is seeking to reconcile the assurance and consulting roles.

b. Even where the auditor is involved in investigations into irregularity, there is still a view that the auditor is primarily examining the circumstances at issue and not the people concerned. Where a name can be fitted to a problem, then this should be a natural consequence of the proceedings much like a witch-hunt. One of the hardest challenges in the audit role is seeking to reconcile the assurance and consulting roles.

c. Even where the auditor is involved in investigations into irregularity, there is still a view that the auditor is primarily examining the people concerned. Where a name can be fitted to a problem, then this should be a natural consequence of the proceedings and not a witch-hunt. One of the hardest challenges in the audit role is seeking to reconcile the assurance and consulting roles.

d. Even where the auditor is involved in investigations into irregularity, there is still a view that the auditor is primarily examining the circumstances at issue and not the people concerned. Where a name can be fitted to a problem, then this should be a natural consequence of the proceedings and not a witch-hunt. One of the hardest challenges in the audit role is seeking to reconcile the assurance and consulting roles.

9.15 Which statement is least appropriate?

Examples of non-verbal communication include:

a. General body movement.
b. Eye contact.
c. Physical position and posture.
d. Touching.
e. Laughter.
f. Hand movement and facial expression.
g. Silences.

9.16 Select the most appropriate example (a, b, c, d, e, f, g, or h) for each type of interview question (1–8):

Interviewees are guided by skilful use of questioning so that material issues are expanded on while specifics are dealt with more quickly. Types of question include:

Question type:	**Example (a–h)**
1. Open questions	
2. Closed questions	
3. Probing questions	
4. Confirmatory questions	
5. Clarification	
6. Leading questions	
7. Loaded questions	
8. Trick questions	

Examples:

a. 'Do you work in the accounts department?'[2]
b. 'I thought you said that you worked for Mr. X?'[5]
c. 'Surely you check these invoices before approving them?'[6]
d. 'Tell me about your job'.[1]
e. 'Tell me more about xyz'.[3]
f. 'You appear to be more qualified than your boss'.[7]
g. 'You say that you have worked here for three and a half years; what date did you start?'[8]
h. 'Your job description refers to a xyz is this correct?'[4]

9.17 Which two statements are least appropriate?

There are several points regarding how audit interviews are conducted that should be noted:

a. The interview should be planned.
b. Auditors should familiarize themselves with the area under review and risk register that are in use.
c. A structure should be aimed at so that there is introduction, fact-finding and winding-up.
d. Observe the requirements of the auditor's code of conduct.
e. Break the ice when starting the interview since a formal mode once entered into will probably be maintained throughout the interview.
f. Formally conclude the interview and do not leave any unresolved matters.
g. Try give the audit opinion on matters raised as this may make the interview more interesting.
h. Formulate specific objectives for the interview.
i. Use negotiation skills where necessary.
j. Ensure that audit brochures are available for the interviewee.
k. One should list all the items that are not immediately available but have been requested by the auditor and this list should be checked at the end of the interview.
l. Avoid taking notes as this might become a hindrance.
m. Watch the human relations aspects and body movement.
n. Above all listen, listen and listen.

9.18 Which statement is least appropriate?

Some of these rules for documenting interviews are:

a. Apply the same documentation standard to all types of interview.
b. Ensure that signatures applied are appropriate to the circumstances.
c. Provide a front summary sheet that contains objectives, results and conclusions that can be reviewed by the audit manager.
d. Use standardized documentation for all interview records.
e. Type the record where necessary whilst retaining the original.
f. Retain documents referred to in the interviews with the record cross-referenced to the point where they are introduced by the interviewee.
g. Apply the usual standards of place, date, time, people present, audit job and reviewed by.
h. Re-read notes for consistency.

9.19 Which two statements are least appropriate?

The main options that the auditor has for documenting the system are:

a. Narrative notes.
b. Block diagrams.
c. Contingency plans.
d. Flowcharts.
e. Testing programmes.
f. Internal control questionnaire (ICQ).

9.20 Insert the missing word/s:

Systems are set out by straightforward ..... where the main parts of the system are noted in bullet points. The processes are described from start to finish to convey the required information on which to base an evaluation. The bulk of these systems notes may be taken direct from the interview with the operations manager. For simple systems that do not involve much document flows, this may be sufficient.

a. detailed flowcharting

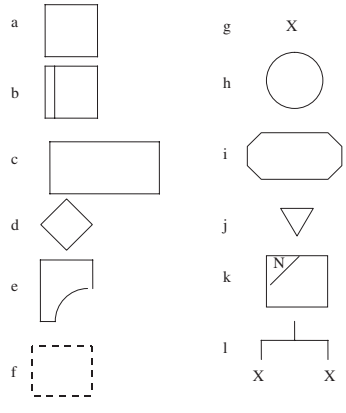
b. narrative
c. computer generated picture diagrams
d. data process flow diagrams

9.21 Which statement is least appropriate?

The rules that are applied to audit flowcharts are:

a. Provide clear headings and dates so that the system dealt with is clearly identified.
b. Do not make them unnecessarily complicated as this consumes time and may not aid the audit process.
c. Look for exception routines and note these so that a complete picture is provided.
d. Test the flowchart against the client's understanding of the system.
e. Distinguish between operations/processes and controls so that the flowchart can feed directly into the control evaluation procedures.
f. Number the events in sequential order as they may be referred to in other audit working papers.
g. Provide extensive narrative notes to aid understanding of the flowchart.
h. Show destination of all documents by not leaving loose ends.
i. Distinguish between information and documentation flow.
j. Use a convention of moving through the system – top to bottom and from left to right.
k. Apply standardized symbols and keys that are fully agreed and detailed in the audit manual.

9.22 Select the most appropriate description (1–12) for each symbol (a–l):

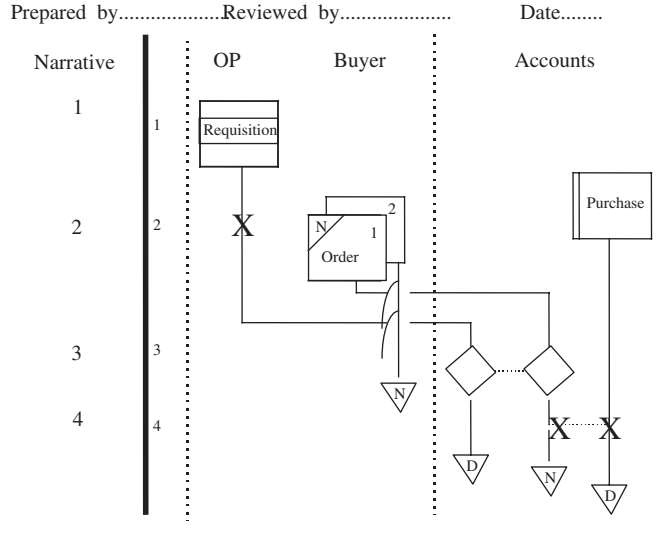


Symbol	Description (1–12)
a.	
b.	
c.	
d.	
e.	
f.	
g.	
h.	
i.	
j.	
k.	
l.	

Select from the following descriptions:

1. alternative process
2. book
3. computer disc
4. computer printout
5. computer process
6. connector
7. control
8. document
9. file
10. ghosting
11. operation
12. pre-numbered document

9.23 Select the most appropriate description (a–d) for each stage of the flowchart (1–4):



Narrative	Description (a, b, c, or d)
1.	
2.	
3.	
4.	

Descriptions:

a. Order prepared
b. Posted to purchase ledger
c. Requisition checked to orders
d. Requisitions passes weekly from main office

9.24 Which statement is least appropriate?

Flowcharts may be used in the following ways:

a. Weak areas or waste of resources may be isolated so that audit attention may be directed towards these parts of the system, or problems can simply be referred to in the report.

b. One can draw a second flowchart to show proposed improvements. The relevant stages may be highlighted in 'before' and 'after' charts that form the basis of discussions with management.
c. One may use the internal control questionnaire (ICQ) in conjunction with flowcharts, expanding on areas where there may be systems weaknesses. ICQs are also a form of systems ascertainment in that they relay the control features of the area under review.
d. Walk-through tests may be used to take a small sample of transactions through the system so that the integrity of the documentation may be determined.
e. Automated flowcharting packages may be used which means the auditor will not have to find out how the system operates.

9.25 What is x?

x ..... may be seen as the most important stage in any audit review since this provides an opportunity for auditors to apply professional creativity to the fullest. The audit opinion and recommendations should flow from the systems weaknesses identified during the systems x ..... Audit testing routines are carried out to confirm the original x ..... in terms of the application of controls and the effects of control weaknesses.

a. ascertainment
b. evaluation
c. compliance
d. review

9.26 Insert the missing words:

We then have to turn to the model of the system that is being evaluated. The system may be conceived as one of several models. Evaluation will be based on ..... although reference will be made to development

a. the prescribed system
b. the alleged system
c. the planned system
d. the emergency/contingency system
e. the ideal system
f. the auditor's preferred system
g. the system that is actually in operation
h. staff's preferred system
i. the workable system
j. the best system

9.27 Insert the missing words:

..... are widely used to assist the control evaluation process and there are many standard packages. They consist of a series of questions applied to a particular operation and designed so that a 'no' answer indicates a potential control weakness.

a. Internal compliance questionnaires (ICQ)
b. Individual control questionnaires (ICQ)
c. Internal control questionnaires (ICQ)
d. Internal check questionnaires (ICQ)

9.28 Which is least appropriate advantage and least appropriate disadvantage?

ICQs have a number of specific advantages and disadvantages:

Advantages

1. Provides a permanent record of the evaluation stage.
2. A disciplined, systematic approach to evaluation not depending on the whims and fancies of the assigned auditor.
3. Helps audit supervisors as the standard of evaluation is set beforehand through compilation of the ICQ.
4. Provides direction to the auditor by setting out clearly the areas that are to be addressed.
5. It is simple to use as the questions are directed at control objectives that should be present in the operation under review.
6. The technique can be used by inexperienced auditors who should find it simple to adapt their work to provide responses to the listed questions.
7. It depersonalizes the audit by setting tried, trusted, and objective criteria for the controls in operation.
8. ICQs promote a systems-based approach and is the only technique that supports this type of review.
9. Provides good structure and form to the audit by defining beforehand the way systems will be assessed.
10. It results in comprehensive cover of an area by dealing with all foreseeable points.

Disadvantages

1. They can lead to a stereotyped approach where each year the auditor seeks to examine a series of predetermined factors that is wholly predictable.
2. It can become mechanical as the task of completing the never-ending checklist becomes so laborious that the auditor develops a secret desire to leave the profession.
3. They may be followed by an auditor who uses the ICQ mainly to focus on the audit work.
4. Detailed ICQs may stifle initiative.
5. Management may feel it is a cumbersome time-consuming technique.

9.29 Which is the least appropriate?

The main headings may appear at the top of the internal control evaluation schedule as:

a. Systems objectives
b. Control objectives
c. Risks to the achievement of control objectives
d. Initial assessment of control weakness
e. Available control mechanisms
f. Existing control mechanisms
g. Initial evaluation of staff absences
h. Testing strategy required
i. Test results
j. Conclusions
k. Recommendations

9.30 Which statement is the least appropriate?

There are several advantages to the internal control evaluation schedule (ICES) approach:

a. It treats controls as part of the process of mitigating risks to achieving objectives therefore it starts with what management is trying to achieve (i.e. the systems objectives).

b. The auditor does not possess an automated answer to controls as suggested by the ICQ approach.
c. The ICES requires the auditor to analyse the system and break it down into logical components as it flows from input, process through to the final output in chronological order.
d. The ICES deals with control risk and exposures as an extension of the evaluation procedure.
e. The ICES flows naturally into the testing routines as after compliance has been reviewed, the poorer parts of the system are then subject to substantive testing.
f. The ICES forms a record of control weakness to be placed in front of management and discussed before the draft audit report is prepared.
g. The ICES is much like the old audit programme approach where a list of basic tasks is given to the auditor to work through.
h. An even better format may be the integrated audit approach where the business advice would embark on a risk workshop to get to the key risks that would then be used to drive the resulting audit.

9.31 Insert the missing words:

During control evaluation the ..... is perhaps the single most important factor and this will be based on experience and training. The whole process of reviewing the system will arise throughout the audit and the formal evaluation techniques may be used to confirm the auditor's initial opinion.

a. perceived system
b. auditor's judgement
c. control perspectives
d. evidence obtained

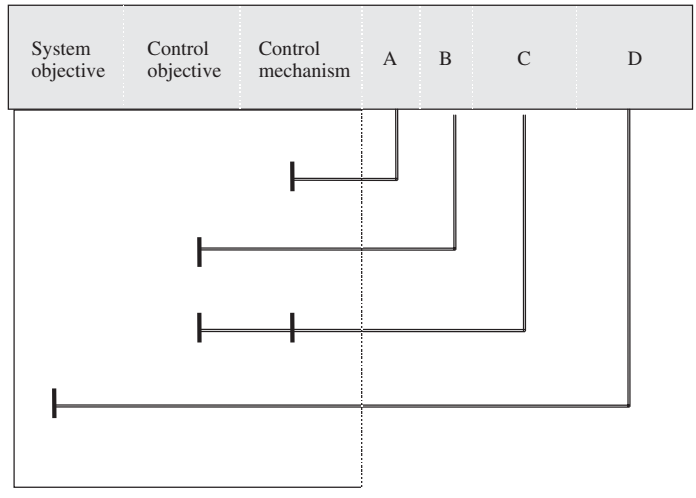
9.32 Which statement is least appropriate?

The testing process involves the following stages:

a. Define the test objective. There must be clear reason for performing the test.
b. Define the testing strategy. How test objectives are achieved is determined by the testing strategy. Formulate an audit programme. The testing strategy can be defined in more detail and form an audit programme of work.
c. Perform the test. The detailed work of performing the tests is the main part of the testing process. Schedule the evidence. The results of testing should be summarized and fed into the report (via the ICES) and be cross-referenced in the working papers.
d. Determine reliability. Set reliability factors for the validity of each test.
e. Interpret the results. The meaning of what is found feeds into the testing strategy.
f. Determine the impact on audit objectives. The link back to the original objectives should be firmly in place so that we take the mass of data and decide what it means for the audit.
g. Determine the next step. Taking into account all that has been found, the direction of the audit should be agreed particularly if there is a need to change plans.

9.33 There are various types of audit tests illustrated as A, B C and D in the Figure below. Select the best description for each of these tests from the choices 1–4:

The various test patterns



Test type	Description (1, 2, 3, or 4)
A.	
B.	
C.	
D.	

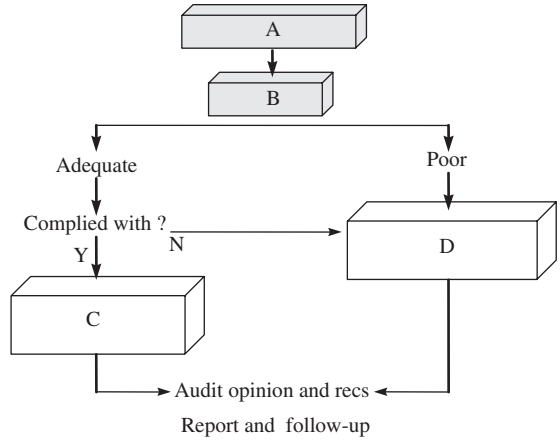
Descriptions:

1. Dual purpose tests check for both compliance and actual error, abuse or inefficiency.
2. Substantive tests seek to determine whether control objectives are being achieved.
3. Compliance tests seek to determine whether control mechanisms are being applied.
4. Walk-through tests seek to determine how the system's objectives are achieved.

9.34 There are various boxes illustrated as A, B C and D in the Figure below. Select the best description for each of these boxes from the choices 1–4:

We restate the systems-based approach to auditing and how these tests fit into the audit process in the Figure below:

Compliance and substantive tests



Box	Description (1, 2, 3, or 4)
A.	
B.	
C.	
D.	

Descriptions:

1. Limited substantive testing
2. Risks
3. Extended substantive testing
4. Controls

9.35 Which statement is least appropriate?

Testing considerations include:

a. The relative risks. The type of risks that arise where a system of control is inadequate or compliance is essential is the most important consideration in testing.
b. Management needs. Where management has concerns about aspects of the system this should feed into the testing strategy.
c. Previous audit cover. The types of findings that were obtained in previous audits can assist planning tests in the latest review.
d. The auditor's own experiences. The auditor may have come across systems in the past where there were certain parts that presented a difficulty.
e. The level of managerial support for the audit. Where there is potential for uncovering sensitive issues that may cause an embarrassment to the organization, these areas may be left out of the testing strategy.
f. The availability of evidence. Testing starts from a hypothetical view of control problems and efforts to substantiate initial findings can look good on paper but be difficult to apply in practice.
g. The audit objectives. Much testing work depends on what one is trying to achieve in line with the stated audit objective.
h. The level of materiality of the item reviewed. Besides dealing with high-risk matters we are also concerned that we take on board materiality.
i. The time available for the tests. The more time available, the more transactions can be tested.
j. The assessment of internal control. This has to be included as the correct answer to the issue of extent and direction of testing.

9.36 Which statement is least appropriate?

Analytical review involves looking at two or more sets of comparable information, say two years' balance sheets, and extracting new data that can be used to direct audit attention towards areas of particular interest. One would be looking for:

a. Changes in key ratios.
b. Absolute changes in key figures.
c. General trends.
d. Findings from previous audits.
e. Movement in the level of purchases and creditors.
f. Movement in the cash and bank account balances.
g. Movement in sales and debtors.

9.37 Insert the missing words:
There are many ways that one can gather the necessary evidence to support the testing objective. The number and types of techniques are limited only by the .....
a. imagination of the auditor
b. time available
c. access to information
d. procedures applied to testing routines

9.38 Which item is least appropriate?
Standard testing Techniques include:
a. Re-performance
b. Observation
c. Corroboration
d. Analytical review
e. Inspection
f. Reconciliation
g. Expert opinion
h. Interviews
i. Assumptions
j. Review of published reports/research
k. Independent confirmation
l. Mathematical models
m. Questionnaires
n. Comparison
o. User satisfaction surveys

9.39 Which statement is most appropriate?
a. The auditor should recognize there is no such thing as 100% perfection in any business system. All systems have some imperfection that results in 'error conditions' discovered through audit testing. These errors may have a significant effect on the performance of the operation and can be tolerated by management. An obsession with these minor infringements can lead to a frustrating audit report that is immersed in the 'findings' without any understanding of the real issues that confront management. Reports that put this into perspective will be better received.
b. The auditor should recognize there is no such thing as reasonable error rates in any business system. All systems have some imperfection that results in 'error conditions' discovered through audit testing. These errors may not have a significant effect on the performance of the operation and can be tolerated by management. An obsession with these minor infringements can lead to a frustrating audit report that is immersed in the 'findings' without any understanding of the real issues that confront management. Reports that put this into perspective will be better received.
c. The auditor should recognize there is no such thing as 100% perfection in any business system. All systems have some imperfection that results in 'error conditions' discovered through audit testing. These errors may not have a significant effect on the performance of the operation and can be tolerated by management. An obsession with these minor infringements can lead to a frustrating audit report that is immersed in the 'findings' without any understanding of the real issues that confront management. Reports that put this into perspective will be better received.
d. The auditor should recognize there is no such thing as 100% perfection in any business system. All systems have some imperfection that results in 'error conditions' discovered

through audit testing. These errors may not have a significant effect on the performance of the operation and can be tolerated by management. An obsession with these minor infringements can lead to a frustrating audit report that is immersed in the 'findings' without any understanding of the real issues that confront management. Reports that put this into perspective will not be well received.

9.40 Insert the missing words:

Testing provides direct material that can underwrite the audit report and conclusions that are contained therein. This is the proper relationship where ..... backs up the action the auditor believes should be taken in seeking to develop better control systems.

a. formal opinions
b. detailed research
c. a formal report
d. the key assumption

9.41 Insert the missing words:

We need to deal with an important development that has growing support and is changing the direction of internal audit. This is the ' ..... ' where the auditor uses automated techniques to examine all relevant data on a database.

a. sample based testing
b. financial testing
c. research-based test result
d. 100% test result

9.42 Which statement is most appropriate?

a. Our audit is not a series of interrogations of information systems but a considered opinion on the adequacy and effectiveness of managerial systems of control.
b. Our audit is not a series of interrogations of information systems but a considered opinion on the adequacy and effectiveness of transaction data.
c. Our audit is not a series of interrogations of information systems but an informal opinion on the adequacy and effectiveness of managerial systems of control.
d. Our audit is not a series of interrogations of information systems but a considered opinion on the adequacy and effectiveness of accounting systems of control.

9.43 Insert the missing words:

..... seeks to establish the degree to which control mechanisms are being applied as prescribed and the results should highlight non-compliance in pursuit of the defined test objective. Often what is meant to happen does not, and procedures that should be in place are ignored.

a. Substantive testing
b. Audit testing
c. Compliance testing
d. Detailed testing

9.44 Insert the missing words:

Systems of internal control operate together and where one part is weak (i.e. not adhered to) then another part may well take over. Auditors may need to look for these ..... controls.

a. unusual
b. compensating
c. compliance
d. internal

9.45 Which statement is most appropriate?

a. Do we need to mistrust everyone and everything? Testing applies the principle of asking what, where, when and why, which is ingrained into the auditor as part of training and experience.
b. Do we need to mistrust everyone and everything? Testing applies the principle of asking what, where, when and why, which is ingrained into the auditor as part of ones intuition.
c. Do we need to mistrust everyone and everything? Testing applies the principle of asking what, where, when, why and who should be blamed, which is ingrained into the auditor as part of training and experience.
d. We need to mistrust everyone and everything: Testing applies the principle of asking what, where, when and why, which is ingrained into the auditor as part of training and experience.

9.46 Select the best description (from choices a, b, c or d) for the attributes of evidence the auditor uses for the audit opinion (1–4):

Attribute:	**Description (a, b, c or d):**
1. Sufficient.	
2. Reliable.	
3. Relevant.	
4. Practical.	

Descriptions:

a. One would weigh up the evidence required, the cost and time taken to obtain it and sensitivity. Some matters cannot be discovered through audit since it would take too much research.
b. The information should be accurate, without bias and if possible produced by a third party or obtained directly by the auditor. The term stimulates images of the evidence being 'dependable, honest, sound, and true'.
c. This ensures that evidence is directed to the control objectives. It brings into play the legal concept of admissibility that requires material to relate specifically to the issues at hand.
d. This is in line with materiality, level of risk and the level of auditors' knowledge of the operation. It means enough, which depends on circumstances.

9.47 Which statement is least appropriate?

Test results will be contained in working papers held in audit files. Working papers should:

a. set out the objectives of the work. All documentation is prepared or secured for a reason and this reason should be defined at the outset.
b. be clear. The working papers should be laid out clearly to promote their use during report writing and review of work.
c. be indexed. The first enclosure of any file should always consist of an index to the papers.
d. support the audit decisions/opinion. Working papers are secured primarily to ensure that audit findings can be justified.
e. use pro formas. One way to promote the use of audit standards in working papers is to use standardized documents.
f. be cross-referenced. Working papers form a whole in that together they tell the story of the audit in terms of work carried out and resultant findings.
g. be economically used. Working papers contain evidence and material relating to the audit.

h. Headed. All documents should contain headers with the name of the audit, date, relevant officers and other details.
i. clearly show any impact on the audit report. Some documents have a profound impact on the audit report while others provide background.
j. be signed by the auditor and the reviewer. It is a practice to place at the bottom of each document, boxes for 'prepared by' and 'reviewed by' along with spaces for the dates.
k. show the work carried out. Documents support the audit opinion and contain matters that may be referred to in the audit report.
l. show the source of information/data. The origins of information in working papers should be clearly defined.
m. indicate which matters are outstanding. A working paper will say what has been done and the results of this work.
n. show any impact on the next audit. The working paper indicates what has been left for later consideration.
o. be complete. There is nothing more frustrating than reviewing a file that suggests that certain items have been missed for no apparent reason.
p. be consistent. Working papers should be wholly consistent. This is important where the audit has been done over a long time period and/or involves several auditors, each dealing with a different part.
q. include full details of documents examined during the audit. Summaries tend not to tell the whole story so all printouts and documentation in that they impact on the audit should be held on the audit file.

9.48 Permanent files contain standing information of a permanent nature while current files record the results of the audit assignment. Note whether the items below belong more to the permanent files (P) or current files (C):

1. Audit review notes.
2. Budgets and other financial data.
3. Committee papers.
4. Any audit programme used.
5. Corporate and operational system notes.
6. Corporate risk register.
7. Internal control evaluation schedules.
8. Management reports.
9. Systems notes and flowcharts.
10. The assignment plan.
11. The system evaluation.
12. Organization charts.
13. The audit report.
14. Previous audit reports.
15. Research items and relevant publications.
16. The objectives statement.
17. Summaries of frauds.
18. The preliminary survey and risk assessment (risk registers).
19. The results of any background research carried out.
20. List of premises and addresses.
21. The scope of the audit.
22. The test results.
23. The testing strategy.

9.49 Which statement is most appropriate?

a. Most auditors need knowledge of statistical sampling and it is advisable to adopt a clear policy regarding use.
b. All auditors need knowledge of statistical sampling although it is difficult to adopt a clear policy regarding use.
c. All auditors need knowledge of statistical sampling and it is advisable to adopt a clear policy mandating its use.
d. All auditors need knowledge of statistical sampling and it is advisable to adopt a clear policy regarding use.

9.50 Which statement is least appropriate?

Advantages of statistical sampling

a. Results may be defended against bias. Bias conjures up images of the auditor being subject to favouritism, narrow-mindedness, one-sidedness and partiality.
b. A defined sample size is provided. A close examination of statistical tables brings out the feature of larger populations requiring only relatively small increases in sample size to meet set parameters.
c. One may safely extrapolate the results and apply them to the wider population.
d. The technique is repeatable and one would expect a similar result from any repetition.
e. It forces one to define and consider the attributes of the population. This means the data in question has to be extensively researched.
f. Computers make statistical sampling more convenient to use. It is simple to ask the computer to generate random numbers.
g. The level of confidence may be predefined. Statistical sampling allows one to define predetermined risk parameters that the final opinion may be set within.

9.51 Select the best description (from choices a, b, or c) for the types of sampling (1–3):

Types of sampling:	**Description:**
1. Judgement sampling.	
2. Indiscriminate sampling.	
3. Statistical sampling.	

a. A predetermined sample size will be provided and one may indicate how reliable and accurate the results are. The auditor has to define the population and set confidence levels.
b. The auditor uses knowledge of systems and people to select items more likely to exhibit certain features. The sample is purposely biased by the auditor to take on board matters that the auditor is aware of.
c. This allows the selection of items at random but is not based on any defined statistical formula. The intention is to secure an unbiased sample although because the sample size is not mathematically based, it is not possible to formally extrapolate the results.

9.52 Select the best description (from choices a, b, c, d or e) for the types of sampling (1–5):

Methods used to define numbers tested are called sampling plans. This section deals with sampling methods and these may be set out as:

Type of sampling:	**Description:**
1. Random sampling.	
2. Stratified sampling.	
3. Cluster sampling.	
4. Interval sampling.	
5. Automated sampling.	

a. This type of sampling may be seen as a selection technique where the auditor uses sampling software to set parameters, determine the number for testing, access the relevant file and then download the selected items into a separate spreadsheet for later analytical testing by the auditor.
b. If we recall that the normal distribution places values in the shape of a bell, then a skewed distribution will not appear symmetrical. This may mean that the auditor can divide the population into several segments that may consist of say a small number of high-value invoices for revenue contracts and a large number of small-value ones for one-off supplies.
c. Here the population should be homogeneous, with no cyclical bias or missing items. If we divide the population size by the sample size then the sampling interval is obtained and every nth item is chosen for testing.
d. This is a convenient way of selecting items for testing where once the number of transactions has been defined, they are then taken from one filing area.
e. This technique is used to select samples such that each item in the population has an equal chance of being chosen.

9.53 Select the best description (from choices a, b, c, or d) for the statistical terms (1–4):
With statistical sampling one has to set the criteria within which the results should be evaluated and this falls under three basic parameters:

Statistical term:	**Description (a, b, c or d):**
1. Error rate.	
2. Confidence.	
3. Precision.	
4. Extrapolation.	

Description:

a. This is the degree to which the results derived from the sample will follow the trend in the actual population.
b. This is the level of error that one may expect from the population being tested.
c. This is when results taken from a sample are grossed up and applied to the whole population.
d. This shows the margin within which the results can be quoted and defines the degree of accuracy that is required.

9.54 For each sampling plan, indicate whether it is best used for compliance testing (C) or substantive testing (S).
The two main types of audit testing are compliance and substantive testing. These two testing conventions require different statistical sampling plans geared into the objectives of the tests. Compliance testing is concerned with specific attributes so that a frequency may be quoted. Substantive testing looks for variables and enables the auditor to quote a range of values from the test results. The sampling plans relate to these types of tests:

Plan:	**Compliance test (C) or Substantive test (S):**
Attribute sampling	
Difference estimates	
Discovery sampling	
Monetary unit sampling	
Stop-go sampling	
Variable sampling	

9.55 Insert the missing figure:

Monetary unit sampling may give the result that out of a population size of £100,000, 60 items should be examined which are selected at intervals of £ . . . . . .

a. 1,000
b. 1,500
c. 1,667
d. 2,000

9.56 Which statement is least appropriate?

Several considerations should be applied when deciding when statistical sampling might be appropriate:

a. Only use statistical sampling where it is appropriate. The auditor makes a conscious decision at this stage rather than an instinctive view that it is not normally used.
b. Define and know the population. Where the technique is applied there needs to be a formal process whereby the item that is being considered is fully researched by the auditor.
c. Ensure that every item has an equal chance of selection. Randomness is a main ingredient of statistical sampling as this supports the objective way that the technique should be applied.
d. Ensure that patterns do not affect the randomness. The population should be capable of supporting random sampling in the way it is formed and maintained.
e. Where judgement sampling is used one may still form definite conclusions about the population. The rules on the application of extrapolation mean precise figures can be projected even where there is no scientific basis.
f. Use an error rate that is reasonable. The error rate is built into the statistical tables and is based on assumptions about the population.
g. Stratify the population where this reduces variability. We have touched upon the position where the auditor wishes to follow a certain line of enquiry, and is hindered by the need to assume a neutral stance by the use of statistical sampling.
h. Do not set needlessly high reliability goals. There are accepted standards that reflect the general business environment.
i. Analyse the results carefully. Statistical sampling is a means to an end and results must make sense and fit the audit objective.

9.57 Which statement is most appropriate?

a. Statistical sampling is not a mandatory technique although it should not be ignored by the auditor as it can be used to comment on a system through the use of a relatively small sample. The audit department should define a clear policy on the use of this technique and where and how it should be applied, and this should appear in the audit manual.
b. Statistical sampling is a mandatory technique that should not be ignored by the auditor as it can be used to comment on a system through the use of a relatively small sample. The audit department should define a clear policy on the use of this technique and where and how it should be applied, and this should appear in the audit manual.
c. Statistical sampling is not a mandatory technique although it should not be ignored by the auditor as it can be used to comment on a system through the use of large samples. The audit department should define a clear policy on the use of this technique and where and how it should be applied, and this should appear in the audit manual.
d. Statistical sampling is not a mandatory technique although it should not be ignored by the auditor as it can be used to comment on a system through the use of a relatively small

sample. The audit department should define a clear policy on the use of this technique and make sure it is always applied, and this should appear in the audit manual.

9.58 Which statement is least appropriate?

Before the full audit report is produced, one would expect interim reports particularly on larger projects. These have several main uses:

a. It forces the auditor to build the report as work is progressed. As such the findings are fresh in the auditor's mind as they appear and are captured in written format.
b. It keeps the audit manager up to date and allows interim reviews of work performed. If the audit has to be aborted or suspended for any reason, then it is possible to report the results to date very quickly.
c. In this way it may be given to the client and so act as a continuous report clearance device as well as bringing the client into the audit process itself.
d. Furthermore, it is possible to produce the final report straight after conclusion of the fieldwork. This approach will also allow audit to comply with the IIA reporting standards that suggest that the report need not be discussed with management.

9.59 Which statement is most appropriate?

a. Executive summaries: A five or six page summary can be attached to the front of the report or issued as a separate document. It provides a concise account of objectives, main conclusions and the steps that management should be taking.
b. Executive summaries: A two or three page summary can be attached to the front of the report or issued as a separate document. It provides a concise account of objectives, detailed findings, main conclusions and the steps that management should be taking.
c. Executive summaries: A two or three page summary can be attached to the front of the report or issued as a separate document. It provides a concise account of objectives, main conclusions and the steps that management should be taking.
d. Executive summaries: A two or three page summary can be attached to the front of the report or issued as a separate document. It provides a concise account of objectives, main conclusions and the steps that audit management should be taking.

9.60 Insert the missing phrase (this phrase applies to both gaps):

Follow-up procedures revolve around the view of ..... where the internal auditor has failed to convince the client management that the risk needs addressing then any associated audit recommendations may not be agreed. Where the internal auditor is convinced that this level of ..... is outside the remit of the corporate risk appetite then the matter should be reported upwards, even up to the board.

a. residual risk
b. outstanding issues
c. inherent risk
d. significant risk

9.61 Which statement is least appropriate?

Audit reports are not published documents but are the result of a comprehensive audit reporting process:

a. Preliminary survey and assignment plan. The audit report can only be started when the planning, fieldwork and analysis of findings has been completed.
b. Clear audit objectives. The next key stage in the reporting process appears in the form of an overall goal.
c. Good audit work. There is very little that can be gained from an audit without ensuring that the underlying work it is based on has been performed to acceptable standards.

d. Client kept involved. Keeping the client up to date and involved in the audit process leads to a better report.
e. Clear well-written drafts. The way a report is written does affect the way the findings, conclusions and recommendations are received.

9.62 Select the best preferred wording (from choices a–k) for the jargonized wording (1–11): One way of ensuring clear reports is to establish a reporting guide and give examples of words that are jargonized (J) and those that are simplified and therefore much preferred (P):

Jargon	**Preferred (a–k)**
1. due to the fact that	
2. endeavour	
3. evaluate	
4. expeditiously	
5. facilitate	
6. finalize	
7. for a period of	
8. for the reason that	
9. generate	
10. have been shown to be	
11. implement	

Preferred words:

a. are
b. because
c. because
d. do, carry out
e. finish
f. for
g. help, ease
h. produce
i. promptly
j. think about, judge
k. try

9.63 Which statement is most appropriate?

a. It must be said that one of the most stressful parts of an audit is the face to face closure meeting that is held once the field work has been completed. Much will depend on the relationship with the client that has been built up during the audit and the extent to which findings have been discussed as they arise. Whatever the scenario, we would hope that the auditor seeks to avoid this stage, as it can interfere with successful reporting.
b. It must be said that one of the most stressful parts of an audit is the face to face closure meeting that is held once the field work has been completed. Much will depend on the relationship with the client that has been built up during the audit and the extent to which findings have been documented in the report. Whatever the scenario, we would hope that the auditor does not seek to avoid this stage, as it is an important component of successful reporting.
c. It must be said that one of the most stressful parts of an audit is the face to face closure meeting that is held once the field work has been completed. Much will depend on the relationship with the client that has been built up during the audit and the extent to which findings have been discussed as they arise. Whatever the scenario, we would hope

that the auditor does not seek to avoid this stage, as it is an important component of successful reporting.

d. It must be said that one of the most stressful parts of an audit is the face to face closure meeting that is held once the field work has been started. Much will depend on the relationship with the client that has been built up during the audit and the extent to which findings have been discussed as they arise. Whatever the scenario, we would hope that the auditor does not seek to avoid this stage, as it is an important component of successful reporting.

9.64 Which two statements are least appropriate?

Audit reports are not published documents but are the result of a comprehensive audit reporting process that may be summarized below:

a. Preliminary survey and assignment plan. The audit report actually starts with a plan that sets the framework for the ensuing audit.
b. Clear audit objectives. The next key stage in the reporting process appears in the form of an overall goal.
c. Good audit work. There is very little that can be gained from an audit without ensuring that the underlying work it is based on has been performed to acceptable standards.
d. Client kept involved. Keeping the client up to date and involved in the audit process leads to a better report.
e. Clear well-written drafts. The way a report is written does affect the way the findings, conclusions and recommendations are received.
f. Effective review process. The key point to the review stage of the reporting process is that this review should ensure that the report is prepared to professional standards, with detailed coverage where this leads to significant delays in releasing the audit report.
g. Positive wrap-up meeting. It must be said that one of the most difficult parts of an audit is the face to face closure meeting that is held if errors have been found.
h. Consultation on the draft. We would next wish to see a formal process whereby the draft report is sent to all parties affected by the recommendations.
i. Oral presentations. It is as well to stage an oral presentation for audits that are more complicated and/or address sensitive matters.
j. Agreed action plans. We arrive at the negotiation/agreement stage that is also part of the reporting process.
k. Final published assignment report. A final report should be prepared along with a clear definition of reporting lines and people who should be given copies.
l. Follow-up. The process is still not complete until we have set up a follow-up routine in line with best audit practice.
m. Quarterly reports. The audit report should feed into the quarterly reporting cycle that seeks to summarize what has been found and reported on in the relevant three-month period.
n. Annual report. The above is equally true for the annual reporting cycle that again should be set within the context of the plan for the year in question.
o. Management action. We arrive at the true audit product in terms of management action based on the audit report.

9.65 Insert the missing word:

A comment from the late Joe Morris made in 1997 is still relevant today: *An internal audit report that talks about . . . . . is no good at all.*

a. problems
b. yesterday

c. management
d. risks

9.66 Which statement is least appropriate?

It is therefore important that the objectives of this final document are clearly established and this may be one or more of the following:

a. To recommend change: The audit report must be first and foremost about securing change in terms of new or improved controls.
b. To provide an insight for management into risk and control issues: It can be said that the audit report will highlight the importance of control issues and relate these to risks to management's own business objectives.
c. To secure action in response to audit advice: Action goes further than recommendation by moving an idea to the status of an actual event.
d. To bring problems to management's attention: Another view of the audit report suggests it is designed to ensure management is aware of unmitigated risk and its effect on systems objectives.
e. To ensure that the results of audit work are clearly documented: Not all audit reports are published and some, particularly preliminary survey reports, are used as internal documents. Others contain no major findings so are not sent out to management.
f. To provide assurance to management on their activities: This part of the role of the audit report is based on the view that audit reviews controls, because they may have fallen into disrepair or misuse.
g. To show managers how their problems may be solved: Pointing the way forward is another objective of the audit report.
h. To provide information about risk management practices: This is a valid objective as many audits will report new information that has been specially developed via the audit process.
i. To protect the auditor: Many reports will have the subsidiary objective of documenting where audit resources were applied and where it was not possible to do detailed work.

9.67 Which statement is least appropriate?

The internal control evaluation schedule (ICES) contains details of each major control weakness that appears as an audit finding in the published report and should include:

a. The operational objective. This is the business objective that is, that which the manager is required to achieve.
b. The operational standard. This provides the control model against which the current arrangements may be measured bearing in mind the fact that audit is about comparing what is, with what should be.
c. The risks of the current practice. This constitutes the supposition that is being tested.
d. The deficiency in controls. This is a concise statement of what is lacking.
e. The cause of the deficiency. Underlying causes must be clearly identified if any progress is to be made in rectifying problems.
f. The effect of the deficiency. Compliance testing is about defining the effect of control weaknesses.
g. Conclusions. An overall audit opinion forces the auditor to consider the wider implications and give a rounded view of the findings.
h. A framework for the recommendations. It is possible to set the boundaries within which recommendations will fall.

9.68 Insert the missing phrase (this phrase applies to both gaps):

The ..... should form a high-level summary of the working papers (properly cross-referenced) that lends itself to being fed directly into the audit report itself. Moreover, relevant material that will enter into the report's standards, findings, conclusions and recommendations will be found in the ..... that promotes a structured approach to drafting the formal audit report.

a. ICES
b. testing schedules
c. interview notes
d. ICQ

9.69 Which statement is least appropriate?

In addition to identifying control weaknesses, the auditor is charged with forming and publishing an opinion based on the audit work performed. This part of the audit report may be based on:

a. the results of control evaluation.
b. the existing control culture.
c. outstanding risk.
d. the underlying causes of basic problems.
e. whether controls are adhered to.
f. whether controls work.
g. the practicalities of available remedies.
h. management's efforts to improve.
i. the effects of any future changes planned.
j. whether audit has done a good job.
k. overall impressions on management's ability and willingness to address residual risk.
l. findings from unofficial sources.

9.70 Which statement is least appropriate?

It is not enough to point out problems without providing guidance on required action. This is the positive part of the audit report and when formulating recommendations, we should consider:

a. the available options. The audit opinion deals with available options in outline by describing different directions management may take.
b. the need to remove barriers to good risk management and control. All audit recommendations are based on securing new resources for management.
c. the exercise of creative thinking. In many audits, managers are aware of control weaknesses and have noted the implication in terms of errors and/or inefficiencies.
d. VFM points. The theory of VFM can be controversial in that some writers argue that it is good systems that will promote VFM.
e. the resource implications of recommended controls. So that the report does not raise more questions than it answers, it is possible to indicate the cost of recommendations.
f. any bad management practices that impair control. It is rare for audit reports to contain attacks on management and this approach sets up confrontation.
g. the ideal solution. The section on control evaluation addresses the concept of the ideal control system.
h. the costs of poor control. Recommended controls are put forward on the basis that the cost of risks, that they are meant to remedy, outweighs the cost of these new/improved controls.
i. practical workability.

9.71 Which two statements are least appropriate?

If work is reviewed as it progresses the draft report will not be delayed awaiting the audit managers' review. The report review may look for:

a. the structure. The report should follow a defined format and reflect what may be called the house style.
b. what the findings are based on. There should be a clear link between the terms of reference, the work carried out, the findings and then the recommendations.
c. how they are expressed. Securing good findings is one consideration but the way they are presented is a separate matter.
d. the tone of the report. One important review point relates to the way the auditors have expressed their findings.
e. gaps. The report must be read as a whole by the reviewer and obvious gaps isolated.
f. the terminology used. The auditor is faced with a dilemma at times where although the line manager will be the main client for the report, it will also be read by others less familiar with the area under review. It is best to aim the report at technical managers who understand the operations that were audited
g. spelling and grammar. This is a material point in that many audit reports contain excellent findings and crucial recommendations but are let down by poor spelling.
h. whether the house style has been applied. Titles, colours, logos, binding and report covers should all follow the adopted format.
i. whether it appears as a professional job well done. The reviewer should ensure that the report reflects a well-done audit that has directed itself to the terms of reference.
j. whether the client would be quite happy to pay for the resources invested in the audit. One interesting feature of the review will be to ask whether the report is worth the cost in terms of audit hours. If not, the report should not be released.

9.72 Insert the missing phrase (this phrase applies to both gaps):

Recommendations must be based on ..... and the extent of this supporting material depends on the importance of establishing the effects of control weaknesses. Where internal auditors are required to attend management working parties which publish reports and make recommendations without comprehensive research then their views should be qualified as not being derived from the normal audit process. The formal audit reports in contrast must be based on ..... that has been derived from the audit process.

a. sound evidence
b. intuition
c. the auditor's knowledge
d. agreed ways forward

9.73 Which statement is least appropriate?

It should be noted that on receipt of a draft audit report the client may exhibit some of the following reactions:

a. What does this mean?
b. Will I lose out?
c. Will I benefit at all?
d. How should I play this?
e. Will this lead to something bigger?
f. Can I use this to get something?
g. Is the auditor manipulating me?
h. Will the auditor discover my false accounting practices?
i. Is there a hidden motive behind all this?

j. What are the costs of getting these recommendations actioned?
k. Can I afford to ignore this report?
l. Will my boss support me?

9.74 Which statement is least appropriate?

The CAE should adopt a suitable policy on responses from the client and they may be:

a. incorporated into the report. Here adjustment is made throughout the report to reflect the comments received from management.
b. built into a management action plan. The important part of the report is the action plan and it is possible to build management's views into this section without making numerous adjustments to the main body of the report.
c. included as an appendix. A convenient method for dealing with responses is to simply include them as an appendix to the report.
d. left out of the report. Present responses as a separate memo that is not included in the report or its appendices.

9.75 Which three statements are least appropriate?

This section summarizes some more features of good audit reports:

a. The client should be thanked for cooperation and assistance through a formal acknowledgement in the report.
b. The report should normally name the managers and operational staff in the area that is audited along with their designated posts.
c. An action plan agreed with management should be set out in the Executive Summary.
d. We should always balance both good and poor features of the area under review so that we are seen to be fair.
e. The client's views should be reflected within the report or their formal response set out as an additional appendix, to ensure that both sides to the audit have been fairly represented.
f. The whole style of the report should be positive and should not consist of a list of basic criticisms.
g. The auditor should never blind the reader with science by using technical gibberish.
h. All reports should be professionally presented.
i. The report should appear fresh and clear so that the reader might enjoy it.
j. All facts should be quoted precisely.
k. One may wish to use the audit 'I' when describing the audit opinion.
l. The required action should be set out in a hierarchy of descending importance with the more important recommendations appearing first along with an appreciation of problems that may face management in implementing them.
m. All excessive detail should be relegated to the appendices.
n. Terms and structures should be consistent and follow logical processes.
o. The work should flow logically with each point building up into a complete picture.
p. Reports should be well presented along with a 'glossy' cover and photographs.
q. The report should be client oriented in that it is directed at the needs of the operational line manager.
r. Reports should be produced quickly and one would expect the audit department to invest in computers, laser printers and a report binding device so that the draft does not spend weeks 'at the printers/typist'.
s. The work should recognize the various constraints that management faces and build these into the recommendations.

t. We should state clearly the objectives, terms of reference and scope of the work and whether these were in fact achieved during the audit.
u. The report must address the real risks facing management if it is to have any relevance to organizational objectives.
v. We must always remember that an ideal position is impossible to achieve and we have to work within the realities of the existing environment.
w. One fundamental truth the auditor must face is that a good audit report is based on the quality of the audit work and liaison with management that has to be done before one is able to report the results.

9.76 Which statement is least appropriate?

When addressing the topic of audit reports it is vital that the auditor understands the actual role of audit. Managers are responsible for their operations and they will retain this right long after the auditor has done the review and deviated to new fields:

a. Auditors should never assume that they know more than management about the particular operation. They are not paid to be experts in any one area.
b. A 'know-it-all' stance is off-putting and can only lead to problems when reporting the results of the audit. The audit must start from management's perspective and what it is seeking to achieve from the operations.
c. Audit is there to 'prop up management' so that managers will continue to require this service from its auditors so as to help improve the organization.
d. Audit is not employed to solve minor managerial problems since audit resources must be directed at material high-risk areas.
e. Audit should not feel that it needs to show managers how to do their job. If management is unable to perform, then this is a control deficiency that needs resolving.
f. Audit should not second-guess management. If management does not know what it is doing, then the underlying causes must be addressed.

9.77 Insert the missing words:

Research has shown that a typical manager will spend only a few minutes on each item of business before turning to another matter. Auditors who cannot identify with this point will find their work for all intents and purposes ignored. Managers may speak of the '. . . . . ' to describe the detailed reports sent out by the audit department that are full of what appears to be insignificant facts and endless testing results.

a. audit impact
b. audit books
c. audit findings
d. audit product

9.78 Select the most appropriate descriptions (from choices a, b, c or d) for the terms (1–4):

Standard 2410-1 states that engagement observations and recommendations emerge by a process of comparing what should be with what is:

Term:	**Description:**
1. Criteria	
2. Condition	
3. Cause	
4. Effect	

Descriptions:

a. factual evidence found during the audit . . .
b. reason for the difference . . .
c. risk or exposure as a result of the condition . . .

d. standard, measure, expectations . . .

9.79 Which statement is least appropriate?

On the topic of ensuring the presentation is well planned and delivered, the following should be noted:

a. Preparation is the key to success. Where the auditor is comfortable with his/her material, we would expect a better performance.
b. Practice makes perfect. Following on from the above, one factor that tends to lower the overall level of anxiety is a foundation of past experience that should make each presentation easier.
c. Eye contact with the audience is essential. Some nervous reactions are based on a fear of the audience who are perceived by the auditor as a potentially hostile group.
d. Muscle tension can be reduced where the muscles are purposely tensed then released.
e. Breathing should be deep as this helps relaxation and so allows the words to flow more freely.
f. The presenter should not move around at all as any movement may increase tension.
g. The presenter must know the subject well. The auditor must have a detailed knowledge of the audit.
h. One may visualize the presenter's role and the objective of getting a message across.

9.80 Which statement is least appropriate?

We have referred to adequate preparations as a key requirement and this will involve:
Notifying the various parties in good time. We will wish to invite the line manager and senior staff in the areas to attend.

a. Setting a clear audit objective. For our purpose we will wish to present the results of the audit so as to introduce the draft audit report that will then be made available.
b. Organizing handouts. Matters that will be referred to that cannot really be included in slides should be given out in advance, or made available at the start.
c. Using visual aids. These should be firmly in place in preparation for the presentation.
d. Selecting a series of examples that may be used to illustrate specific points. These should be taken from the audit and should consist of findings that were derived from testing.
e. Administrative arrangements so that delegates are not inconvenienced. Coffee, biscuits, maps, handouts, seating arrangements and other administrative matters should be part of the preparation.
f. Time should be carefully planned and rehearsals help clarify this. Although, at the start of the presentation it is not a good idea to indicate how long the presentation should take, as this will mean any overruns may be criticized.
g. The level of technical competence of the audience should be determined and the presentation format directed accordingly. The managerial level should guide the detail provided.

9.81 Which statement is most appropriate?

a. Some auditors see questions as flash points where possible confrontation may arise. The usual motive for questions is a search for more information on specific issues and this is the whole point in having presentations, where feedback can be generated. To avoid these questions defeats this objective. Where a delegate is seeking confrontation the person should be made to feel inadequate.
b. Some auditors see questions as flash points where possible confrontation may arise. The usual motive for questions is to apply as much pressure as possible for the presenter. To avoid these questions defeats this objective. Where a delegate is seeking confrontation the person may be asked to meet separately to discuss any specific problems.

c. Some auditors see questions as flash points where possible confrontation may arise. The usual motive for questions is a search for more information on specific issues while the whole point in having presentations is to impart information and not generate feedback. To avoid these questions defeats this objective. Where a delegate is seeking confrontation the person may be asked to meet separately to discuss any specific problems.

d. Some auditors see questions as flash points where possible confrontation may arise. The usual motive for questions is a search for more information on specific issues and this is the whole point in having presentations, where feedback can be generated. To avoid these questions defeats this objective. Where a delegate is seeking confrontation the person may be asked to meet separately to discuss any specific problems.

9.82 Which five statements are least appropriate?

Practical considerations when conducting the presentation are:

a. Anticipate questions and ensure full answers are provided. Some auditors see questions as flash points where possible confrontation may arise.

b. Ensure that eye contact is avoided with the audience. It is more effective to include all in the room by looking at each person from time to time.

c. Move around in a controlled fashion and use the various facilities properly. The slide show may be used to focus the presentation.

d. Speak clearly and do not repeat what has been set out on a slide. This not only retains control but avoid irritating those who may feel the slides are boring.

e. Negotiate and do not assume a fixed position where reasonable points are raised. The auditor should not engage in heated discussion but must rise above the emotions present.

f. Ensure that working papers are available for detailed queries although we may defer the response if further research is required. Give overview answers but defer more detailed ones.

g. Relax and watch out for nervous gestures which distract. Playing with keys or a watch creates an annoying distraction and this can become obsessive behaviour if left unchecked.

h. Control the audience but do not attempt to move them along when a point has been dealt with. Most people recognize when one person is overreacting or making too many enquiries but they tend to object if the auditor tries to move them along.

i. Audit presentations are about bringing to management's attention the problem, its cause, the effect and required changes. This can be done quickly and effectively where the facts are explained and brought to life.

j. Managers are entitled to assume risks where no action is taken although the implications should be carefully set out. As long as they understand the significance of audit recommendations then management takes full responsibility for them.

k. Professional presentations lift the audit image and get management on audit's side. The auditor looks impressive even if the presentation is not well planned.

l. We may use the opportunity to educate management in both the role of internal audit and the importance of effective risk management and internal control. The questions and answers part of the presentation can be used to sell the audit product and pass over ideas to management such as self-audit.

m. We may place alternatives in front of the management and the resulting feedback may make evaluation and the final decision easier. Negotiation skills come to the fore although it is not wise to simply throw away major audit findings as might occur if this is taken to the extreme.

n. Questions should not be encouraged since a noisy audience may indicate that the presentation has not been a success. If questions are left unanswered or unasked then management and audit may deal with them later on.
o. Generally the burden of proof falls on internal audit since management will not take action or redirect resources unless for good reason. It is part of the audit role to persuade them by constructive reasoning.

9.83 Insert the missing word (it is the same for each gap):
There is no point in convening a ..... where the relationship between internal audit and the client is impoverished or has broken down. The ..... then becomes point scoring with little constructive work possible. There is nothing to be gained from a ..... where the underlying audit has not been professionally done. Where findings are flawed, recommendations unworkable and/or the auditor has not been objective, the work cannot be defended in a .....
a. presentation
b. working party
c. project
d. negotiation

9.84 Which statement is least appropriate?
The quarterly reports will tend to include:
a. Planning and control matters for the audit department. This will explain whether there are issues and developments that affect the scope and effectiveness of the audit function now and in the near future.
b. An outline of audit's performance for the quarter. This provides results of performance indicators that measure quality and quantity of audit work.
c. Statistics on types of work performed and departments charged which will indicate the work that has been performed over each main Department/Section.
d. Detailed extracts of audit reports issued. These extracts should show the terms of reference, work carried out, findings and recommendations for each audit completed during the quarter.
e. Details of staff turnover. Information concerning starters, leavers, training programmes and exam success, transfers and any skills' gaps should be included since it may have a direct impact on the audit plans.
f. Overall productivity per output within time budgets. This will be based on achieving the quarterly plan, the monthly plan and the requirements of the assignment plan.
g. Many are now seeking to assess internal audit's performance in terms of outcomes rather than outputs.

9.85 Which two statements are least appropriate?
Key points relating to the annual audit report:
a. The annual report must be received by the highest levels of the organization, ideally a suitably constituted audit committee.
b. Comments relating to particular audits should be based on both draft and final audit reports.
c. Where the annual reporting period has expired then the annual audit report should only address issues relating to the previous year.
d. Performance data covering internal audit should be based around comparing actual results to planned targets.

e. A view on the overall state of risk management and internal controls (possibly over the main key control areas) should be expressed along with the main implications of any material weaknesses and how these might then be tackled.
f. A suitable format for the annual report should be decided beforehand.
g. The annual report will be formed more at an overview level.
h. Problem areas encountered over the year.
i. Pensive thoughts on the current state of the audit function and barriers to good performance.

References

1. Sawyer Lawrence B. and Dittenhofer Mortimer A., Assisted by Scheiner James H. (1996) *Sawyer's Internal Auditing*, 4th edition, Florida: The Institute of Internal Auditors, p. 221.
2. Flesher Dale (1996) *Internal Auditing: A One-Semester Course*, Florida: The Institute of Internal Auditors, p. 149.
3. Burley-Allen Madelyn (1995) *Listening – The Forgotten Skill*, New York: John Wiley and Sons Inc.
4. Johnson Gene H., Means Tom and Pullis Joe 'Managing conflict'. *Internal Auditor*, Dec. 1998, pp. 55–59.
5. Novak Mike 'Door number three'. *Internal Auditor*, Dec. 1997, pp. 55–57.
6. Moeller Robert and Witt Herbert (1999) *Brink's Modern Internal Auditing*, 5th edition, Para. 7.1, New York: John Wiley and Sons Inc.
7. Sawyer Lawrence B. and Dittenhofer Mortimer A., Assisted by Scheiner James H. (1996) *Sawyer's Internal Auditing*, 4th edition, Florida: The Institute of Internal Auditors, p. 333.
8. *Evening Standard*, 30 Oct. 2002, pp. 8–9, 'My undercover diary of shame', Millar Chris.
9. Hubbard Larry 'Audit working papers'. *Internal Auditor*, pp. 21–22.
10. Colbert Janet L. 'Audit sampling'. *Internal Auditor*, Feb. 2001, pp. 27–29.
11. Sawyer Lawrence B. and Dittenhofer Mortimer A., Assisted by Scheiner James H. (1996) *Sawyer's Internal Auditing*, 4th edition, Florida: The Institute of Internal Auditors.
12. Anderson Urton and Chapman Christy (2002) *The IIA Handbook Series: Implementing The Professional Practices Framework*: IIA, p. 167.
13. Bossle Francis X. and Michenzi Alfred R. 'One page audit report'. *Internal Auditor*, April 1997, pp. 37–41.
14. The Word Centre (1999) *Plain English Writing Guide*: Cabinet Office.
15. Kennedy Gavin and Brealey Nicholas (1998) 'The New Negotiating Edge, the Behavioural Approach for Results and Relationships', London.
16. *Daily Mail*, Tuesday 30 Oct. 2001, 'We're getting the right message (4,000 times every day)', Kendall Paul.
17. Morris Joe, *Internal Auditing*, Sept. 1989, p. 19.
18. Ridley Jeffrey 'Mind your language'. *Internal Auditing and Business Risk*, Jan. 2001, p. 13.
19. Bromage Mary C. (1984) *Writing Audit Reports*, 2nd edition, New York: McGraw-Hill, p. 1.
20. Warburton Nigel (1996) *Thinking from A to Z*, London: Routledge.
21. Mandrel S. (1987) *Effective Presentation Skills*: Kogan Page.
22. Baldwin Alan 'Better than a thousand words'. *Accountancy Age*, 23 Mar. 2000.
23. Ziegenfuss Douglas E. 'Measuring performance'. *Internal Auditor*, Feb. 2000, pp. 37–40.
24. *Internal Auditing and Business Risk*, Oct. 2002, p. 31.
25. Internal Auditing & Business Risk, IIA Magazine, June 2009, pp. 22–25, 'Fraud special report', Arthur Piper.
26. Internal Auditing & Business Risk, IIA Magazine, June 2009, p. 28, 'Fraud special report', Self Defence, Neil Baker.
27. Managing the Risk of Fraud, 'The Red Book, CIPFA Better Governance Forum', Chartered Institute of Public Finance and Accountancy, Oct. 2006, p. 1.
28. A CIO's guide to IT risk management: tapping the extraordinary potential for business value and financial growth, IBM Sep. 2008, p. 3.
29. Internal Auditing & Business Risk, IIA Magazine, Closing the gap, Antony Ruddenklau and Peter Westberg, Sep. 2007, p. 20–23.
30. INFOSEC Research Council (IRC), 'Hard Problem List', Nov. 2005.
31. Internal Auditing & Business Risk, IIA Magazine, Aug. 2009, p. 38 'Finding the weakest link', Nick Huber.

32. John Buchanan tells Neil Baker what he looks for in a head of internal audit, Aug. 2009, pp. 27–31, Anthony Garnett (Chairperson of CHEIA, Council of Higher Education Internal Auditors and Head of Business Assurance, Durham University).
33. Senior Supervisors Group, 'Risk Management Lessons from the Global Banking Crisis of 2008', 21 Oct. 2009, p. 4.
34. Internal Auditing & Business Risk, IIA Magazine, Sep. 2008, pp. 34–36, 'The write stuff?' Arthur Piper.
35. Hubbard Larry D. 'What's a good audit finding?'. *Internal Auditor*, Feb. 2001, p. 104.

Chapter 10

MEETING THE CHALLENGE

Introduction

Our final chapter provides a brief account of some of the challenges for the profession based on comments from writers from the internal audit community and beyond. Note that all references to IIA definitions, code of ethics, IIA attribute and performance standards, practice advisories and practice guides relate to the IPPF prepared by the IIA in 2009. The areas that are touched on include

10.1 The New Dimensions of Internal Auditing
10.2 The Audit Reputation
10.3 Globalization
10.4 Examples
10.5 Meeting the Challenge
Summary and Conclusions
Assignments and Multi-choice Questions

10.1 The New Dimensions of Internal Auditing

We accept that internal audit must deliver added value to the organization and this is defined by the IIA as:

> Value is provided by improving opportunities to achieve organizational objectives, identifying operational improvement, and/or reducing risk exposure through both assurance and consulting services.

Against this measure is the changing face of internal auditing which is summed up in the IIA's work in the context of internal auditing competency frameworks, in Chapter 5 of the IIA Handbook Series on 'Implementing the professional practices framework':

Past Focus	Additional Focus
hard controls	soft controls
control evaluation	self-assessment
control	risk
risk	context
risk threats	risk opportunities
past	future
review	preview
detective	preventive
operational audit	strategy audit

auditor	consultant
imposition	invitation
persuasion	negotiation
independence	value
audit knowledge	business knowledge
catalyst	change facilitator
transaction	processes
control activities	management controls
control	risk
consciousness	consciousness[1]

This sets the new dimensions for internal auditing where the concepts on the right-hand side become a benchmark for each chief audit executive to consider.

10.2 The Audit Reputation

There is a view that the organization of the future will revolve around its reputation and that the so-called chief risk officer will become the chief reputation officer. In turn, the internal audit shop will have to consider its own reputation and what it means to the organization. William E. Chadwick has considered the importance of the audit image:

> Internal auditors should be proud of the contributions they make to the internal controls of an organization. Unfortunately, they rarely receive the recognition they deserve, because their accomplishments often are overshadowed by the bad news they must impart. Therefore, it is important for internal auditors to educate their clients on the value of internal auditing and build relationships that can withstand a negative audit. Using humor is a great way to begin that process. Internal auditing doesn't have to be doom and gloom. Auditors need to let the world in on this well-kept secret and, at the same time, improve their image and enhance communication with their clients.[2]

The internal auditor helps drive and is driven by the corporate governance agenda. In the past, auditors would define their role and responsibilities by considering what they would most enjoy doing and what fitted their skills base. Nowadays, the internal auditors can only really view their role by reference to societal expectations and the challenge is inherent in the ability to judge how business and public services will develop. The audit role shadows what is happening in the wider world and the words of Sir Adrian Cadbury, interviewed 10 years on from the ground-breaking Cadbury review of corporate governance, provide a guide to the way the governance agenda is maturing:

> He makes an unlikely enforcer. A tall patrician, immensely courteous and very English retired businessman of the old school, Sir Adrian Cadbury is a world away from the slicked back aggression of grandstanding US prosecutors. Yet this septuagenarian toff, author of the Cadbury Code, is in demand around the world for the advice on taming the wilder excesses of freewheeling capitalism. His ground breaking report has given Britain an enviable reputation as the cradle of the modern corporate governance revolution. He is truly the Codefather.
>
> December 1st marks the tenth anniversary of Don Cadbury's epic. Like the Marlon Brando movie, it has spawned a series of sequels, the Greenbury and the Hempel thrillers, with a fourth, Higgs: the report, currently in post-production.

The Cadbury report – officially the Financial Aspects of Corporate Governance – was commissioned by the accounting bodies and the Stock Exchange in 1991 against a background of financial chicanery that has many echoes in today's post-Enron world. Two company collapses – in particular the furnishing and wallpaper group Coloroll and Asil Nadir's bizarre conglomerate Polly Peck – had raised serious concerns in the city because almost nothing of the true nature of their precarious positions was revealed in their accounts.

As Sir Adrian and his fellow committee members rolled up their sleeves, two far more serious financial bombs exploded – the BCCI banking scandal and the Maxwell pension raid. Suddenly what had started as a little noticed and a rather academic exercise took on a far greater significance. Nothing less than London's reputation as a financial centre of probity was on the line.

The result was a report that provoked howls of protest from much of the business establishment. The fears now, with the benefit of ten years' hindsight, appear ludicrously Luddite. The CBI whined that the code would lead to the introduction of 'foreign style' two-tier boards. One business body went as far as to condemn it as 'a draconian remedy'. Others complained that it would do nothing to deter dishonest bosses. A decade on, its two page Code of Best Practice has become a sort of Ten Commandments of the business world. While non-compliance with its 19 voluntary recommendations is not actually a sin, companies that do flout the code are regarded as raffish at best and with deep suspicion at worst. Ideas that upset so many in business a decade ago – full disclosure of directors' pay and the division of chairmen and the chief executive roles – have long since taken on 'motherhood and apple pie' status. Only a handful of quoted company bosses – John Ritblat at British Land is one of the best known – still hold on to both top roles.

Sir Adrian believes a Voluntary Code has served Britain well and worries that the current hysterical 'something must be done' mood post-Enron will spawn more prescriptive, possibly even statutory, regulation that will not improve corporate governance standards. 'I think a very clear example of the problem of trying to regulate statutorily is the great question of whether you should split the post of chairman and chief executive,' he says.

Where the chairman is also the chief executive, it is essential that there is a strong independent element on the board with a recognised senior member. Sir Adrian says 'if you said there is now a law that Maxwell must have a chairman if he is going to remain chief executive, all he would have done is appoint a puppet. In answer to any question from share holders he would have said: "I've done what the law lays down, I've satisfied the regulation." Whereas with our formulation that there must be a clearly accepted division of responsibility at the head of a company, investors can go on asking, well what is the division?'

The 'box ticking' approach in America contributed to the wave of scandals that has shaken confidence in the US capitalism, he says.

In the Enron case the questions the board asked were 'does it get past our legal counsel, and secondly, will the auditors wear it?' Therefore you got these special purpose entities and a whole bunch of financing cons because the board felt as long as they had put it against these two tests, the law and the auditor, that it was OK. Of course really what the board should have been saying is 'what are the risks of what we are doing, is it actually sensible business?' Not 'is it legal, will the auditors pass it?'

Sir Adrian is particularly concerned that Derek Higgs, the former Warburg banker who is heading an inquiry into the role of the non-executive directors, will be pressured into recommending cast-iron rules for Britain. He says 'What I worry about is that there will be pressure on Higgs to come up with rules on things like the number of boards anybody can sit on. In my view, it

simply is not the right way to do it. I'm sure Higgs will look at things thoroughly objectively and sensibly but the political pressure all the time is always to be seen to be doing something.'

He points with dismay to the hasty reaction to the corporate governance crisis in America, where this summer's Sarbanes Oxely Act forces chief executives and chief financial officers to sign off their accounts every quarter and threatens a maximum penalty of 20 years' imprisonment if they prove to be false. '20 years in jail is also the maximum penalty for the attempted murder of a witness', he says.

Are there areas of corporate life that are still worrying Sir Adrian a decade on from the code? Inevitably, the vexed issue of the directors' pay is high on the list. He says 'The remuneration committee should look at the structure of the remuneration throughout the company not just the pay of the directors at the top. It should ask, is there a logical pay structure from the top to the bottom because the pay at the top is contributed to by the rest of the company? I don't have any objection to high pay provided it is the result of a well thought out scheme related to performance. The criticism has been, and it is rightful criticism, of high reward without high performance or even worse, reward for failure.' He also feels chairmen should take their share of responsibility: 'In the first instance the blame lies in appointing people you then have to dispense with.'

According to Sir Adrian, the challenge for remuneration committees 'is designing pay and bonus systems which are first of all firmly tied to observable performance, and secondly are reasonably medium term, if not long term. What pension funds want, what investors want, is continuing progress, not a great surge and then a falling back.'

So how does he now look back on the effectiveness of the Code? Could it, for example, help prevent an Enron or a WorldCom in Britain? 'It's more difficult. The accounting standards would not allow that off-balance sheet financing for a start and I think the extraordinary business of putting your chief financial officer in charge of a special purpose vehicle which was trading in the assets of the company – I cannot see that being acceptable. There will always be crooks; there will always be a Maxwell type.'

'All you can do is say that the accounting standards have got to be tight, auditing has got to be effective and there has got to be disclosure so you make it more difficult. It will be very foolish to say that these things can't happen, but it would be difficult.'

'If you go back to Maxwell, the Board of Trade inquiry had said he was not fit to head a public company. But people still went on his board and the banks still lent him money in a big way. You can narrow the possibilities – but you can never eliminate them.'[3]

10.3 Globalization

One real development in internal auditing coincides with the way businesses (and public services) are becoming increasingly internationalized. Physical location is no longer an issue because buying activity is moving away from the local high street as it launches into hyperspace through the Internet. The IIA has grasped this new thinking and is developing the profession into a global internal auditing organization whose broad business objectives include:

- establishing global standards for the practice of internal auditing;
- promoting the professional certification of internal auditors worldwide;
- fostering the development of the profession around the globe;
- representing and promoting internal auditing across national borders;

- facilitating the timely sharing of information among member associations;
- searching for globally applicable products and services.[4]

There has been further activity in Europe to bring like-minded professionals together. Neil Cowan (past president IIA. UK and Ireland and past vice president ECIIA), director general ECIIA 1999–2002, has described the European scene for *The Internal Auditing Handbook*:

> The profile of professional internal auditing received a significant boost when, at the beginning of the millennium, the European Union (EU) established a separate Directorate General for Internal Audit (DGIA). At the same time, an independent Audit Progress Committee was set up. Together, these innovations reflected a new determination in the EU to drive forward a more effective approach to matters of audit, risk and control. These moves also encouraged further development of internal auditing in member States where the profession was already well established and gave further impetus in countries where less developed approaches were evident.
>
> All of this was a recognition at European level of the contribution that professional internal auditing can make to good governance, not just within the EC itself, but also in countries throughout the wider European geographic area. Given the depth of involvement of the EU in all areas of economic activity, this was also a signal that the benefits of internal auditing were available to all types of organisations in every economic sector.
>
> Staffing of DGIA sought to reflect the right professional qualifications required to undertake a value adding internal audit service. A prime requirement also was the acceptance of global internal auditing standards in order to establish an effective benchmark. By this example, the EC sought to provide a lead for EU member States in establishing their own approach to the provision of assurance on the application of good governance principles, risk management and internal control. Many EU member States actively encourage internal auditing in the knowledge that this service to management provides a valuable contribution to public confidence in the way in which organisations in both the public and private sectors are governed. However, countries may differ in the role which is expected of internal auditing and the means by which the service is provided. Some countries seek a confirmation from internal audit that controls are effective in the financial area only whilst others see internal audit as a full partner with an organisation's Board and management in providing assurance over effective governance processes which embrace risk assessment and operational control.
>
> In some EU member States the professional body for internal auditors – the Institute of Internal Auditors (IIA) – has been long established, is a crucible for driving the profession forward and promotes the adherence to the IIA Standards for the Professional Practice of Internal Auditing. These countries are involved in the debates about the way in which firms and other organisations operate and are a full party to developing laws and regulations in appropriate areas of activity. In other countries which have not reached this level of professional development, the IIA assists in raising standards and promoting professional practice.
>
> Professionalism of the internal auditor is the key factor in providing risk and control assurance to Directors and Management Boards. Skill, knowledge, ability and experience – and, thus, credibility – are reflected in the qualifications that an internal auditor can bring to an organisation. Whether directly audit related, or generally in business, the qualified internal auditor is part of the comfort factor which Boards seek in gaining assurance over effective management processes. Other factors should come from an effective Audit Committee.
>
> A well constituted Audit Committee of the Board, made up of independent non-executive Directors, should challenge the Board in its approach to good governance. The Audit Committee

role should be to provide an oversight of risk management and internal control activities and advise the Board where problems may occur. The Committee should seek meaningful input from both internal and external audit and should be instrumental in providing the Board with on-going control information in addition to having significant influence over the Board's annual control statement.

The internal audit function, together with an effective Audit Committee, provide two significant pieces of the corporate governance jig-saw puzzle. Separately they can make a strong contribution to effective corporate governance; working closely together they become formidable.

10.4 Examples

Professor Jeffrey Ridley has described the new-look internal auditor with reference to the following factors:

- Competition – For all auditing (and assurance) services it will increase. Study the marketing of services by all professional firms – not just auditing! Learn from their 'selling' skills. Market your internal auditing services as a business . . .
- Objectives – Have a clear sense of internal auditing purpose and values that everyone understands . . .
- New business – Keep up to date with research into internal auditing practices and use this knowledge to experiment, develop and market your future services (also products).
- Technology – Up to date technology will be the key to all internal auditing best practices in the future . . .
- Regulation – Understand the authority, responsibilities and activities of inspectors and regulators in your own sector, and that of your suppliers and customers . . .
- Outstanding – Do not just 'do your best' or be 'excellent', be 'outstanding' . . .
- Learning – Be part of the new learning age . . .
- Standards – Search for relevant and appropriate external standards and codes of conduct for all operations you audit. Test against these standards and codes.[5]

Philip Sainty has described a survey conducted by the institute in the wake of the WorldCom debacle, concerning the way the internal auditing profession has moved away from traditional financial auditing towards risk-based auditing. Four groups were described in terms of attitudes towards this change:

- **The Evangelist:** Some 48% of respondents fell into this group. They believed that the move towards risk-based auditing has not had a negative impact on the traditional work of internal audit and should continue unfettered.
- **The Doomsayer:** Some 24% of respondents fell into this group. They believed that the move towards risk-based auditing has damaged the traditional work of internal audit and should not continue.
- **The Pragmatists:** Some 18% of respondents fell into this group. They felt that the move to risk-based auditing had changed the traditional work of the internal audit, but said that the trend should continue nonetheless.
- **The Doubters:** Some 5% of respondents fell into this group. They felt that the move to risk-based auditing had not damaged the traditional work of internal audit but said that the trend should not continue.[6]

We stated at the start of the Handbook that it is important not to throw the baby out with the bathwater. Professor Andrew Chambers has warned about the dangers of getting swept away on the tide of consulting styles and not retaining a semblance of our original role, by suggesting that:

> I am a bit of a traditionalist. Rather than looking for some jazzy, sexy new horizon to strive for (as has been internal auditors' wont since the start), my view is that the pendulum may swing back. Someone has to provide the good old fashioned assurance through control assessment (including detailed testing) comprehensively covering all the affairs of the enterprise over time. When will managements and internal auditors learn! Boards are already convinced, I think – they know the importance of assurance.

10.5 Meeting the Challenge

All countries to a greater or lesser extent are coming to recognize the great value from an internal audit service. It is hard to think of any particular corporate service that is enshrined in laws and regulations and which carries the burden of the societal expectations that we have mentioned. Keeping to the international theme, we can quote an example from the complementary Listing Requirements of the Malaysian Stock Exchange, which describes the value from internal auditing:

- Reviewing objectives and activities – review with management the operational activities and ensure the principal objectives are aligned to overall company's objectives.
- Evaluating risk – identify all auditable activities and relevant risk factors, and to assess their significance.
- Confirming information – research and gather information that is competent, factual and complete.
- Analysing operations – analyse and examine that operations are effective.
- Providing assurance on compliance – provide assurance on compliance to statutory requirements, laws, company policies and guidelines.
- Recommending internal controls – recommend appropriate controls to overcome deficiencies and to enhance company operations.
- Assuring safeguards – evaluate procedures in place to safeguard company assets.
- Consulting and facilitating – assist management in establishing a proper risk management framework, assessing risks and monitoring the effectiveness of the risk management programme and ensuring the adequacy of the internal control system.[7]

The new-look internal auditor will have a view on whether ERM has been implemented and will help this task wherever possible. What sounds simple in theory can be very difficult in practice, as one senior manager in charge of over 50 staff recounts the demands and tensions created by a focus on customer service:

> We have talked about the importance of a commitment to effective systems of control from the senior management of an organisation. It is fine for senior management to say it is committed to effective internal controls and then ask line managers to prepare and sign formal certificates that controls have been put in place to minimise identified risks. Top management in turn, ask their front line staff to provide assurances regarding the effectiveness of these controls. It can become worrying when that same senior management team do not insist on compliance with all procedures when faced with high levels of varying demands from customers and stakeholders. This is when the importance of formal systems of internal control versus an ad hoc response to

meeting service demands becomes evident. It is not uncommon, in a service-based operational environment, for customer service needs to conflict with official procedures. This sends mixed messages to staff who perceive that management place a degree of importance on formal controls only when they need to certify that controls are being applied. Junior staff are often very knowledgeable about risks to a business and become cynical about senior management's commitment to managing identified risks, when the goal posts are continually moving. Moreover risk management is now being increasingly devolved to front line teams. Most employees need to know about corporate governance and risk management. In reality, many managers and supervisors are placed in defined risk management roles with little or no idea of their responsibilities in this area. It is unfair to expect untrained and unaware managers to effectively manage risks to a business.

Providing Audit Assurances

The task of providing reliable assurances has never been more crucial to the internal auditing profession. There are several key issues that underpin the need to ensure internal auditors are able to step up to the plate and not only discharge their professional duties but also fill a gap in the governance framework, where the captains of industry need to be sure that all is well below decks. The CAE will need to consider the following five questions:

1. What is the state of the audit shop and is it fit for the purpose?

IIA standard 2120 says that 'the internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.' Practice Advisory 2120-2 acknowledges the expectations on internal audit to deliver the goods and deal with the high level of risk facing high profile internal audit units. An interesting question arises as to how internal audit is able to take the necessary steps to ensure that it is managing its own risks. Advisory 2120-2 argues that risks facing internal audit fall into three broad categories: audit failure, false assurance and reputation risks. Some of the steps the CAE can consider are summarized below:

- quality assurance and improvement program;
- periodic review of the audit universe;
- periodic review of the audit plan;
- effective audit planning;
- effective audit design focused on understanding the system of internal controls;
- effective management review and escalation procedures;
- proper resource allocation.

The above forms a high-level system of internal control over the internal audit unit and as a beacon for good control the CAE should ask for assurances from the audit managers that each of these controls is in place and working. As part of the 'physician heal thyself' syndrome, the CAE will want to prepare a risk register that caters to key risks to the audit service and ensures a continual review of the accepted controls and other arrangements to promote a successful audit function.

2. To what extent does the audit service fit into and enhance the corporate assurance map?

If the primary role of internal audit is to provide independent assurances on the risk management, control and governance process, then these assurances need to fit into the assurance map. Practice Advisory 2050-2 comes to the rescue by explaining how standard 2050 is met in

terms of coordinating the activities of other internal and external providers of assurance and consulting services to ensure proper coverage and minimize duplication of efforts. Advisory 2050-2 acknowledges that the board will want to gain assurance from the various sources that processes are operating properly by suggesting that there are three main classes of assurance providers, differentiated by the stakeholders they serve, their level of independence from the activities over which they provide assurance, and the robustness of that assurance:

1. those who report to management and/or are part of management (management assurance), including individuals who perform control self-assessments, quality auditors, environmental auditors and other management-designated assurance personnel;
2. those who report to the board, including internal audit;
3. those who report to external stakeholders (external audit assurance), which is a role traditionally fulfilled by the independent/statutory auditor.

These assurance providers include:

- line management and employees
- senior management
- internal and external auditors
- compliance
- quality assurance
- risk management
- environmental auditors
- workplace health and safety auditors
- government performance auditors
- financial reporting review teams
- subcommittees of the board
- external assurance providers, including surveys, specialist reviews (such as health and safety).

The advisory makes it clear that the internal audit activity will normally provide assurance over the entire organization, including risk management processes which include how key risks are classified and the effectiveness of the risk assessment and risk reporting systems.

3. How does the internal audit plan ensure the best use of audit in providing relevant assurances?

Most agree that the CAE will use the risk management process to drive internal audit plans.

Practice Advisory 2010-2 covers the way this may happen. The advisory recognizes that internal auditors may not be qualified to review every risk category and the ERM process in the organization (e.g., internal audits of workplace health and safety, environmental auditing or complex financial instruments). Factors the internal auditor considers when developing the internal audit plan include:

- Inherent risks – Are they identified and assessed?
- Residual risks – Are they identified and assessed?
- Mitigating controls, contingency plans and monitoring activities – Are they linked to the individual events and/or risks?
- Risk registers – Are they systematic, completed and accurate?
- Documentation – Are the risks and activities documented?

In addition, the internal auditor coordinates with other assurance providers so as to be able to identify different kinds of activities to include in the internal audit activity's plan, including:

1. control reviews/assurance activities
2. inquiry activities
3. consulting activities.

Many organizations have developed risk registers that document risks below the strategic level, providing documentation of significant risks in an area and related inherent and residual risk ratings, key controls and mitigating factors. An alignment exercise can then be undertaken to identify more direct links between risk 'categories' and 'aspects' described in the risk registers and, where applicable, the items already included in the audit universe documented by the internal audit activity. An internal audit activity's plan will normally focus on unacceptable current risks where management action is required.

4. Does our audit work build into a high-level assurance service?

Most auditors are used to planning an audit, doing field work and preparing a report with a formal opinion. What is less straightforward is how to align this audit work into macro-views that can be applied to large parts of the organizations, major business processes and in terms of the implications for key risks to the organization. The IIA's Practice Guide on formulating and expressing internal audit opinions was brought out in April 2009 and this highlights some of the issues that internal audit may need to give opinions on, covering, for example:

- the overall system of internal control over financial reporting;
- organization controls and procedures for compliance with laws and regulations;
- effectiveness of controls such as budgeting and performance management in multiple subsidiaries;
- system of internal control at a subsidiary or reporting unit;
- compliance with laws and regulations in a single business unit or a few business units.

The guidance suggests that stakeholders also need to understand the nature of the opinion that it covers, the criteria used to express the opinion and the time period in question. It goes on to show how macro opinions need to be expressed with care to make sure the user understands the purpose, the basis of the opinion, the risk appetite used by the organization and the work done to support the opinion, including reliance on others. These types of opinions may result from the aggregation of different audits each carried out at different times, although micro opinions are easier as they are based around an individual audit. In essence, the framework against which the opinion is set is very important as this gives the context for the work and results. Negative opinions result where nothing has come to the auditor's attention that causes concern. The work of the third party assurance provider needs to be assessed for competence, independence and objectivity before it can be relied on by the internal auditor. The practice guide gives examples of the way in which some audit units use a tiered grading of controls as:

- effective
- some improvement needed
- major improvement needed
- unsatisfactory.

Opinions can be given on the areas that have been audited but there is still a need to consider the way audit work contributes to the overall assurance map. We can return to Practice Advisory 2050-2 for guidance on the way in which an assurance mapping exercise can be used to map assurance coverage against the key risks in an organization. This process allows an organization to identify and address any gaps in the risk management process and gives stakeholders comfort that risks are being managed and reported on, and that regulatory and legal obligations are being met. Organizations will benefit from a streamlined approach, which ensures the information is available to management about the risks they face and how the risks are being addressed. Each significant unit within an organization could have its own assurance map. Alternatively, the internal audit activity may play a coordinating role in developing and completing the organization's assurance map. In organizations requiring an overall opinion from the CAE, the CAE needs to understand the nature, scope and extent of the integrated assurance map to consider the work of other assurance providers (and rely on it as appropriate) before presenting an overall opinion on the organization's governance, risk management and control processes.

5. How do we move the internal audit function forward?

There is so much to chose from when considering developments in the future positioning of the internal audit. We can start with the work carried out by PricewaterhouseCoopers in their work, 'Internal audit at a crossroads: Choosing a new strategic path':

> As organizations consider new techniques to manage risks and controls, our study suggests they will look to both internal audit and other functional areas to assess risk as well as to perform the more traditional assessments of controls. Spurred by Sarbanes-Oxley and other reform measures, organizations have taken steps to strengthen controls and expand their controls-related monitoring activities. As a consequence, the value ascribed to traditional controls-focused assurance activities will likely diminish and potentially erode some of the newfound stature that many internal audit functions have attained in recent years. As other risk management functions assume new responsibilities in areas such as controls (and, in the process, enhance their value in the eyes of management), internal audit, with its strong association with controls assurance, could be perceived as being limited in its ability to deliver comparable value. Internal audit thus finds itself at a crossroads, with two possible paths to the future. One is to continue doing what it does today and nothing more, a path that brings with it the inherent risk of future obsolescence. Alternatively, internal audit may choose the path we believe is more likely to lead it to meet the evolving needs of modern organizations, and the rising expectations of senior management and audit committees. This path involves moving beyond the fundamentals of risk and controls to create a new internal audit value proposition. The new (and inherently more strategic) value proposition would include the provision of risk management assurance along with the traditional responsibility of assurance over controls. Adding risk management capabilities would inevitably help internal audit align itself more closely with an organization's maturing risk management functions. But doing so would require something not always associated with today's internal audit function: a risk-centric mindset.[8]

One major concern is how the internal auditor should act if the risk appetite applied in the organization is acceptable or excessive. What does the auditor do when confronted by reckless behaviour? The chief risk officer may also have a view in this situation. There is a big difference between smart risk taking and reckless risk taking. New challenges for internal audit revolve around the theme of daring to go into danger zones, as well as safe areas. One such danger zone is pay and incentives and even bonuses. One huge risk pops up where bonus systems incentivise

the wrong set of behaviours and it is here that internal audit can step into areas of corporate controversy. Jonathan Watson has described this issue, via the European Commission's stance:

> Jean-Nicolas Caprasse, head of European corporate governance research for RiskMetrics Group's ISS Governance Services unit, welcomed the Recommendations. "The wording is quite strong," he says. "The Commission has chosen to act through Recommendations, which are not binding, because the alternative of drafting a Directive is a much longer process. It seems that they wanted a quick impact. They plan to monitor things very closely and intervene if necessary." Caprasse believes that it is high time for internal auditors to get more involved in companies' approach to pay, both in the financial services industry and elsewhere. "A number of parties need to do a better job of monitoring each other to help companies find their way out of the current crisis," he says. "Internal auditors need to get involved in providing their own assessment to management of the risk level of underlying pay packages. Pay policies and procedures are defined by the board or the supervisory board, and internal audit needs to ascertain whether pay packages comply with those policies and procedures. They might not assess the level of risk inherent to specific remuneration provisions – that is more the responsibility of the remuneration committee, maybe using advice from remuneration consultants – but the internal audit function needs to ascertain that this is actually being put into practice, not only for top executives but also for risk-taking staff like traders." Time for the bullet-proof suit? The European Commission wants internal auditors to get more involved in assessing company pay strategies in the financial sector.[9]

We can turn next to solid supporters of the internal audit role in the form of Professor Mervyn King, chairman of South Africa's 'King Committee' on corporate governance, who opened the 2008 IIA conference:

> ... with a rousing call for internal audit to take its rightful place in "the boardroom, not the backroom". In an address titled "Governance, strategy, sustainability and internal audit", King argued that the role and status of internal audit was changing because boards were demanding greater assurance on strategic issues. "Two years ago I said the profession would be changed completely within five years and so far I have been proved right," he told delegates. Internal audit can no longer be divorced from strategy, he continued. "Internal audit has to be involved with management in developing strategy, otherwise how can you know whether controls are adequate, that the quality of corporate information is such that the non-execs and the board can have confidence in relying on it?" "Strategy is the board's responsibility," he stressed, "but who is in a better place to understand the risks and opportunities in developing that strategy than internal audit? I believe no one." Internal audit was becoming a risk-centred and "intellectual" discipline, said King, adding: "The days of internal audit being compliance centred are dead forever."[10]

At the IIA UK & Ireland's annual conference there was continued support for risk-based auditing:

> Outgoing Institute president Simon D'Arcy told delegates that the profession had come a long way in recent years, but needed to change yet further if it is to meet boardroom expectations. "We must consolidate our progress by future-proofing, honing our communications skills and constantly thinking about what we are doing, in order to give the quality of assurance required by senior management," he said. D'Arcy outlined what he called "intelligent internal auditing". This did not mean esoteric or "boffinlike" auditing, he said. "It means thinking about what you are doing." Internal auditors should adopt a risk-based approach and make sure they provide

> "assurance around things that really matter," otherwise their value to their organisation is open to question. This is particularly true in the current economic climate, where financial firms are collapsing under the burden of unforeseen or badly assessed risks, he said.[11]

It is one thing to ask for a seat at the top table and quite another to ensure you get invited back. IIA standard 1111 takes internal auditing way beyond the old days of checking accounting records and physical inventories by stating that the CAE must communicate and interact directly with the board. This interaction will include committees, such as the audit committee and risk committee set up by the board and in terms of reinforcing this most important relationship practice advisory 111-1 provides some much needed guidance:

> Direct communication occurs when the chief audit executive (CAE) regularly attends and participates in board meetings that relate to the board's oversight responsibilities for auditing, financial reporting, organizational governance, and control. The CAE's attendance and participation at these meetings provide an opportunity to be apprised of strategic business and operational developments, and to raise high-level risk, systems, procedures, or control issues at an early stage. Meeting attendance also provides an opportunity to exchange information concerning the internal audit activity's plans and activities and to keep each other informed on any other matters of mutual interest. Such communication and interaction also occurs when the CAE meets privately with the board, at least annually.

One key interaction is where the CAE challenges the board on whether key risks are being adequately addressed. The sticking point is whether management and internal audit agree on the way this is happening and when there is a gap, standard 2600 swings into action:

> When the chief audit executive believes that senior management has accepted a level of residual risk that may be unacceptable to the organization, the chief audit executive must discuss the matter with senior management. If the decision regarding residual risk is not resolved, the chief audit executive must report the matter to the board for resolution.

The acceptance of risk and the resolution gaps between the opinion of internal audit and the views held by senior management will be the question that all chief audit executives will face now and in the future. In one sense, this will define the audit role – as when all is well, the auditor can be a trusted advisor but when there is a problem, this role turns into one of a critical friend. The adopted approach comes back to the question of risk appetite and how it can be used to drive the risk governance agenda is one challenge that will not go away. Deloittes has a view on how we can use a series of key questions to assess the risk appetite within an organization:

- What size risks or opportunities do we expect management to bring to our attention?
- How does management determine the organization's risk appetite? Which risk categories are considered, and how do they relate to management's performance goals and compensation metrics?
- In developing the risk appetite, how did management incorporate the perspectives of shareholders, regulators, and analysts – and experiences of peer companies?
- How are risk tolerances set? How does that process account for risk appetite? How do risk tolerances relate to the risk appetite and to risk categories?
- What scenario-planning or other models are used in setting the risk appetite and tolerances? How do these tools account for changing circumstances and for the human factor?[12]

Ernst & Young go on to describe their research into areas where there is room to improve risk management in most organizations:

- Improving the risk assessment approach to better anticipate, identify and understand risks
- Aligning risk management focus with business objectives to drive greater value and focus on the risks most likely to affect the business.
- Enhancing coordination of risk and control groups to achieve greater efficiencies and eliminate redundancies, duplication and gaps among risk activities Organizations that improve their risk management activities will not only provide better protection for their businesses, but also improve their business performance, improve their decision making and, ultimately, increase their competitive advantage.[13]

It is important to coordinate the various risk and control groups and it is here that internal audit needs to step up to the plate. The question is, are we just another risk and control group? Or can we rise above the rest and ensure our job is to review the way risk is managed including the way these risk and control groups help drive and improve the agenda? The examination of challenges facing the internal audit profession will not be complete if we do not refer to the proposition of Professor Andrew Chambers that these challenges call for a new breed of 'Super Auditor':

> The enhancement of the internal audit role I am suggesting will need the development of a cadre of "super auditors" with requisite skill sets and accreditation mechanisms. Outsourced assistance to the internal audit function is likely to become even more important. CAEs will need a status and a quality equivalent to that of an executive director, and they will be held more to account for any failures to provide timely warnings to the board. In medium to large internal audit functions there will need to be a mezzanine level of internal auditors, immediately below the CAE, also able to interface on equal terms with members of the board. We will need to reconsider the continued applicability of the term "chief audit executive", which implies an affiliation to the management team. I notice I am not alone in thinking along these lines. Indeed, if internal audit is not to fill the board's assurance vacuum, other professionals probably will. BBC's Today programme on October 30, 2008 reported that Paul Moore, head of regulatory risk at HBOS from 2002 until he was made redundant in 2004, considers that "people like him need to report direct not to executive management but to non-executives whose job it is to rein in management." In the age of the sound bite, the idea of the "super auditor" resonates strongly. Of course, I am keen to engage in consideration of whether and how the board's assurance vacuum needs to be filled, and the other changes to internal audit, in addition to the fostering of super auditors, that will be needed if the internal audit profession is to rise to this latest challenge.[14]

One of the most important developments during 2009 is a slight change of wording applied in internal auditing standards from 'should' to 'must'. There is no hiding place and each audit shop across the world will need to ensure it is able to stand up to the rigours of the IIA's International Professional Practices Framework, as it asks that the standards are applied by setting out clearly what it means when a requirement is a 'must':

> The *Standards* use the word "must" to specify an unconditional requirement.

A final word in this section comes from Sarah Blackburn, who presents a serious challenge to all internal auditors across the world:

> People sometimes concentrate on the outputs of internal audit: the reports, the recommendations, the advice given. But the value to stakeholders is the outcome – ultimately they feel more confident because of what internal audit is telling them. If the audit committee and the board are confident that the regulator will be satisfied and that management's assurances and the risk management process are sound, they are more likely to undertake new opportunities to grow the business and achieve more stretching goals.'[15]

Summary and Conclusions

There is much that internal audit is expected to contribute and much that can be done to make this contribution. In August 2002, LeRoy E. Bookal, chairman of IIA.Inc., wrote that:

> With our unique viewpoint as independent but inside observers, internal auditors play a vital role within governance processes by keeping the board, senior management, and external auditors aware of risk and control issues and by assessing the effectiveness of risk management . . . Audit committees and boards are facing skyrocketing liability costs and ever-increasing workloads. It's no wonder that liability costs are rising – boards have to meet more governance challenges each year, but their resources for information about their increasingly complex organisations are limited. In the post-Enron era, it is surprising that boards of directors for any publicly held companies would choose to do without internal auditing. It is also surprising that investors, liability insurers, and other stakeholders have not questioned the decision to do without internal auditing more often . . . There is no simple checklist showing everything internal auditors can do to add value, because, at times, techniques for adding value are as unique and personalized as the organisations for which we work.[16]

We have featured the words of Larry Sawyer in the Handbook and there is no reason not to include something in the final chapter. Many years ago, Sawyer wrote out Ten Little Maxims for the internal auditor:

1. Leave every place a little better than you found it.
2. You can't stomp your foot when you are on your knees.
3. Know the objectives.
4. Nothing ever happens until somebody sells something.
5. Every deficiency is rooted in the violation of some principle of good management.
6. Never believe what the first person tells you.
7. The best question is, 'Mr. or Ms. Manager, how do you satisfy yourself that . . . ?'
8. Politics and culture will usually win over rules and regulations.
9. When you point your finger, make sure your finger nail is clean.
10. Murphy was an optimist.[17]

When an auditor is considering an operational risk during an assignment, but cannot see the big picture in relating this task to the top boardroom corporate governance agenda, regard should be given to a famous poem by George Herbert:

For want of a nail the shoe is lost;
For want of a shoe the horse is lost;
For want of a horse the rider is lost;
For want of a rider the battle is lost;
For want of the battle the kingdom is lost.

My view of the changing world of the internal auditor is quite simple, and it is summed up in the following dimensions that move through stages 1–7; from old- to new-look contexts:

1. We're here to check on you
   2. We're here to check your controls
      3. We're here to check your risks
         4. We're here to check your risk management system
            5. We're here to help you establish risk management
      6. We're here to help you protect your business
   7. We're here to help you prove you can be trusted to take care of our business
8. We're here to support the way you grow the business in a way that is entirely sustainable.

The late Professor Gerald Vinten was involved in the first edition of *The Internal Auditing Handbook*, and it is only proper to give Gerald the final say in all matters of internal audit:

> In the quarter of a century I have been associated with internal audit, the profession has come on leaps and bounds. Indeed the existence of this extensive Handbook, plus the fact that already it is in a second, revised edition, is witness to this progress. The Foreign Corrupt Practices Act in the USA was one significant milestone, but much more significant was the more recent Turnbull report in the UK. This is the case since with the American Act, although internal audit was one route to achieve the objectives of the Act, internal audit was not placed quite centre stage or in its rightful context. Fraud and corruption detection and prevention are worthy achievements, but they are scarcely capturing the essence or raison d'être of a business or organisation. With the Turnbull report internal audit has reached total maturity, and excelled itself. It is placed in its rightful context of corporate governance, strategic management and internal control. I am pleased to be associated with the internal audit profession, to have been the President of the Institute of Internal Auditors – UK and Ireland, and to continue to see this Handbook go from strength to strength. In the uncertain world in which we are living, the accounting profession has much to be guilty of. Internal audit, on the other hand, has carried itself with decorum and integrity. My poem (see Appendix C) attempts to reflect this.

Chapter 10: Multi-choice Questions

10.1 Insert the missing word (this word applies to all three gaps).
There is a view that the organization of the future will revolve around its ..... and that the so-called chief risk officer will become the chief ..... officer. In turn, the internal audit shop will have to consider its own ..... and what it means to the organization.
   a. compliance
   b. reputation
   c. control
   d. performance

10.2 Insert the missing name.
The late Professor ..... has provided an enlightening poem (Appendix C of the Handbook) to reflect the view that, in the uncertain world in which we are living, the accounting profession has much to be guilty of. Internal audit, on the other hand, has carried itself with decorum and integrity.
   a. Henry Vinten

b. Gerald Vinny
c. Gerald Vinrose
d. Gerald Vinten

References

1. Chapman Christy and Anderson Urton, IIA 2002 'Implementing the professional practices framework', p. 91, in The IIA Handbook Series.
2. Chadwick William E.'Oh no the auditor is here'. *Internal Auditor*, April 2002, pp. 52–55.
3. Prynn Jonathan, 'The Codefather'. Reproduced with kind the permission of the *Evening Standard*, Friday 29 Nov. 2002, pp. 44–45.
4. Global IIA, The Case For Globalization, 1 Oct. 2001 (www.theiia.org).
5. Professor Ridley Jeffrey 'A new internal auditor for a new century'. *Internal Auditing*, Jan. 2000.
6. Sainty Philip, 'Breaking out'. *Internal Auditing and Business Risk*, Sept. 2002, pp. 19–20.
7. Guidance on internal audit function, task force set up by the Securities Commission of Malaysia, IIA Malaysia acted as Secretariat to the Task Force, Complement KLSE Listing Requirements – Malaysia, July 2002.
8. Advisory Services Internal Audit, connectedthinking, Internal Audit 2012, A study examining the future of internal auditing and the potential decline of a controls-centric approach. p. 5, 2007 PricewaterhouseCoopers LLP.
9. Internal Auditing & Business Risk, IIA Magazine, PAGE June 2009, Jonathan Watson.
10. Annual Conference Special, Internal Auditing Magazine, pp. 38–47, November 2008, The Institute held its annual conference in September. Neil Baker and Arthur Piper report.
11. Annual Conference Special, Internal Auditing & Business Risk, IIA Magazine, pp. 38–47, November 2008, The Institute held its annual conference in September. Neil Baker and Arthur Piper report.
12. Risk Intelligent governance, A practical guide for boards, p. 9, Risk Intelligence Series, Issue No. 16, 2009, Deloitte Development LLC, Member of Deloitte Touche Tohmatsu.
13. The future of risk: Protecting and enabling performance, p. 3, Ernst and Young 2009.
14. Internal Auditing & Business Risk, IIA Magazine, December 2008, p. 21, Andrew Chambers.
15. Internal Auditing, Decemeber\January 2009, p. 15, Sarah Blackburn, Presendent of the IIAUK & Ireland.
16. Bookal Leroy E., Chairman of IIA.Inc. 'Internal auditors – integral to good corporate governance'. *Internal Auditing*, Aug. 2002, pp. 44–49.
17. Sawyer Lawrence B., 'An internal audit philosophy'. *Internal Auditor*, Aug. 1995, p. 46.

Appendix A

INDUCTION/ORIENTATION PROGRAMME

There is no one way to provide induction for newly appointed internal auditors. The method chosen will suit the organization and internal audit shop in question in line with the overall corporate policy on induction. New audit staff may enter the audit shop and be taken under the wing of a coach or mentor who will oversee the way this person adapts to the new environment. Or the new starter may be placed on a formal orientation programme and engage in training seminars, and/or formal staff conferences. In some organizations, the new person is thrown into the audit team and given smaller jobs to start with, and perhaps some one-to-one development with a more experienced auditor. There is no right or wrong way of going about this task. This appendix is based on *The Internal Auditing Handbook* being a resource that represents basic minimum knowledge that all audit staff should possess. It is also based on a simplistic model of induction where the main activity involves giving the new starter the Handbook to work with for a few weeks. This can work so long as it is supplemented by a close personal contact between the new starter and the designated audit manager and the rest of the audit team. The two-week induction programme that utilizes *The Internal Auditing Handbook* is based on the new starter (referred to as Auditor X) arriving on Monday morning and finishing the programme on the second Friday:

Monday

New starter (Auditor X) arrives and is given the usual introductory tour, shown the audit manual, plans, sample reports, etc. After this, Auditor X may be taken through the way the induction programme will operate as well as receiving a copy of *The Internal Auditing Handbook* and is asked to work through Chapter 1 at work (and also encouraged to read at home).

Tuesday

Auditor X is asked to work through the rather larger Chapter 2 of *The Internal Auditing Handbook*.

Wednesday

In the morning, Auditor X undergoes an hour-long written test based on several assignment and multi-choice questions taken at random (excluding question ten) from Chapter 2 of the Handbook. After which Auditor X is asked to work through Chapter 3 of the Handbook.

Thursday

In the morning, Auditor X undergoes an hour-long written test based on several assignment and multi-choice questions taken at random (excluding question ten) from Chapter 3 of the Handbook. After which Auditor X is asked to work through Chapter 4 of the Handbook.

Friday through to the Following Thursday

The above is repeated for Chapters 4 to 9 (Chapters 1 and 10 do not contain related questions), which takes us to the ninth day (Thursday).

The Final Friday

Each of the final questions for Chapters 2 to 9 involve the preparation of a presentation to the Internal Audit Management Team (IAMT). Auditor X will be told on the final Friday morning which chapter (question 10) to study in preparing the relevant presentation. This presentation will be made after lunch to the IAMT (or whoever is available) and consist of two parts. The first is the delivery of the chosen question, and the second is a general session where Auditor X describes some of the things that have been learnt during the two-week induction programme, and will be asked to offer any relevant suggestions for improving the way induction is undertaken (this becomes a form of simplified audit and delivery of audit opinion performed by Auditor X). The Internal Audit Management Team will be supportive and encouraging and keep an eye open for 'high flyers' and those that will need further development. Where multi-choice questions are used to test the new auditor during the induction program, make sure the auditor does not have access to the suggested answers at Appendix E.

(Note – the website stay-in-control.com may be used as an additional training tool for auditors and other staff.)

Appendix B

CRSA BEST PRACTICE GUIDE

What Makes for a Good Process and Conversely What are the Common Mistakes Made

By Paul Moxey of the UK's CRSA Forum

Introduction

The sinking of the *Titanic*, the failure of Enron, the near collapses of Equitable Life and Marconi and the rail disasters which killed people and resulted in the de-privatization of Rail Track are all examples of failure, by businesses, to manage risk. CRSA is a powerful tool to help management manage risk and when done well can also have a dramatic effect on organizational effectiveness.

All organizations operate in environments that create uncertainty, and this uncertainty often leads to risk. Risk management enables organizations to deal more effectively with uncertainty, and reduce the likelihood or impact of adverse events and increase the benefit from favourable events.

Over the last ten years, managing risk is getting increasing attention. This is partly a response to many spectacular corporate failures and is probably also a result of 're-engineering' – the restructuring which occurred in many organizations where layers of management were removed and management controls lost. While 'risk management' in one form or another is as old as mankind, traditionally it focused on managing risks arising during specific activities. What is new is the emphasis on enterprise or business risk. Here risk is being looked at from a holistic perspective across the whole organization and considering strategic risks as well as operational risks.

Risk can be defined in many ways and there is a degree of controversy in risk management circles. Confusingly, risk managers often give the word a different meaning from that found in dictionaries. One American authority defines it as the possibility that an event will occur and adversely affect the achievement of objectives, another (Australian/New Zealand) defines it as something, measured in terms of consequences and likelihood, happening which will have an impact on objectives. The latter definition presupposes that risk can be an opportunity to be exploited as well as a bad thing to be avoided or minimized. Many risk managers are keen to widen the definition of risk to include opportunities. Most dictionaries, however, only define risk in negative terms. There is no authoritative business definition of risk in the UK but the Turnbull guidance on internal control and risk management uses the word 'risk' only in a negative context.

Organizations are managed through a combination of formal and informal controls. Formal controls tend to be controls which have been designed by management for a particular purpose. Examples include written policies, authorization procedures and separation of duties. Informal control is harder to evaluate and is not necessarily the result of conscious management design, it

includes things like culture, teamwork and communication. Formal controls are what management would like to happen, informal control determines what actually happens, which formal controls are bent, ignored or followed. Traditionally risk management, and audit, have focused on evaluating formal controls yet corporate failures, without exception, result from breakdown of informal controls.

Best Practice

Ideally risk management should be embedded into normal management rather than be an 'add on'. Organizations work best if everyone in them is aware of their objectives, the risks which exist and acts accordingly.

CRSA is probably the most effective way of embedding risk management and of assessing informal control. CRSA involves assembling teams in structured workshops. In a workshop, a team can consider their organization's and their team's objectives and then consider what risks are present and how they should be managed. All people manage risk as part of their daily lives, in and out of work, yet usually they do so without thinking consciously of their objectives or risks. Many people do their jobs without ever considering risk or even what their objectives are. A well-run workshop results in a better shared understanding of a team's objectives and the risks that are present. It helps build a consensus on how risks should be managed and in what priority. It can often also result in improved teamwork, communication and therefore a more effective or successful team. A common comment after a risk management workshop is 'that was the best team meeting we have ever had'.

My experience as a facilitator has taught me not to be surprised when the board of an organization is vague about the organization's objectives. It is then almost a certainty that teams lower down will be even more unclear about what they are there to do. A CRSA workshop requires people to consider their objectives as a group, this in itself results in the team having a better clarity of purpose which means a better chance of achieving these objectives more effectively.

There is no single right way of running a CRSA workshop but a few general principles are worth bearing in mind:

- A workshop depends on people expressing themselves openly. It is therefore important to ensure that people feel comfortable discussing important issues. It is a good idea at the beginning of a workshop to establish agreement to preserve confidentiality. It is also important to enable quieter people to contribute. This can be achieved by enabling people to contribute in other ways than simply speaking. Most people are happy to express thoughts on Post-it notes, this has the added advantage of being almost anonymous as other people will be writing too rather than looking at somebody else writing. Electronic voting methods can also be very useful although are by no means essential.
- A facilitator needs to establish rapport with the workshop. A good way of doing this is simply by allowing the workshop to talk (or write) about what is important to them. One can ask, for example, what concerns the group has about its ability to achieve their objectives.
- A workshop works best when the energy is flowing and the mood positive. A risk of risk management workshops is that too much attention on what can go wrong saps people's enthusiasm and energy and creates an atmosphere of helplessness. Such an atmosphere kills team spirit and motivation to address problems. A simple but effective way to keep people positive is to ask them what strengths the group has that helps them in achieving their objectives.

This usually gets the group very positive and feeling empowered to tackle problems they might otherwise have given up on or left to more senior management.

- A framework such as COSO or CoCo provides a very useful basis for assessing control.
- Finally, a facilitator should have a clear idea of what the workshop should achieve but be as passive as possible during the workshop. The facilitator provides the structure but must leave the content to the group. A facilitator should speak as little as necessary and keep his/her opinions to him/herself.

The Future of CSA and How We Can Keep the Initiative Moving Forward

The corporate governance debacles of 2001 and 2002 have highlighted the importance of informal control and having the right cultural tone at the top. Traditional audit methods can offer little in assessing such things. CRSA has a great deal to offer. A well-run workshop is the best way of assessing informal controls.

A workshop is uniquely effective in considering ethical issues in an organization. Enron could never have happened if a CRSA workshop programme had been embedded across the organization. An Enron culture could not have existed in an organization committed to workshops. Conversely, the Enron culture would probably have prevented CRSA from working. If a board tries CRSA and finds it does not work it may be an indicator of a serious problem.

While an organization or team can assess informal control, the assessments are subjective. This does not diminish the value of the assessment for a workshop but many managers and auditors are instinctively uncomfortable with any process which does not generate hard numbers. This can mean that some are oblivious to the benefits of the workshop.

Recent corporate events have created an appetite for certainty and precision on assessing the effectiveness of control or vulnerability to risk. Unfortunately this is a discipline where certainty and precision are not possible and are unlikely ever to be so. Managers need to learn to work with what is available from a workshop, which is a wealth of qualitative, rather than quantitative, information. Most workshops generate numbers but these are always based on subjective assessment and should be regarded as indicative rather than black and white.

If management can accept and work with these limitations then CRSA has the potential to be not just the most effective tool for risk management but also a powerful strategy tool.

The Contribution of the CRSA Forum

The CRSA Forum has been in existence since the mid-1990s and meets quarterly. It is a network of CRSA practitioners and others interested in CRSA. The Forum is informal and members use the forum to discuss their approach to CRSA and learn from each other. The forum exists to:

promote the value and benefits of CRSA in corporate governance and enterprise risk management
share diverse approaches and experiences
identify and develop best practices
provide a resource for CRSA users
acting as a catalyst for new ideas
collaborate with relevant professional bodies

Its mission is:

> Sharing, progressing and promoting best practices in self-assessment of enterprise risk management and control in all organisations.

The forum welcomes new members and is happy to assist those new to or considering using CRSA for the first time. For further details contact www.accaglobal.com/crsa.

Appendix C

A POEM BY PROFESSOR GERALD VINTEN

In the quarter of a century I have been associated with internal audit, the profession has come on leaps and bounds. Indeed the existence of this extensive Handbook, plus the fact that already it is in a second, revised edition, is witness to this progress. The Foreign Corrupt Practices Act in the USA was one significant milestone, but much more significant was the more recent Turnbull report in the UK. This is the case since with the American Act, although internal audit was one route to achieve the objectives of the Act, internal audit was not placed quite centre stage or in its rightful context. Fraud and corruption detection and prevention are worthy achievements, but they are scarcely capturing the essence or *raison d'être* of a business or organization. With the Turnbull report internal audit has reached total maturity, and excelled itself. It is placed in its rightful context of corporate governance, strategic management and internal control. I am pleased to be associated with the internal audit profession, to have been the President of the Institute of Internal Auditors – UK and Ireland, and to continue to see this Handbook go from strength to strength. In the uncertain world in which we are living, the accounting profession has much to be guilty of. Internal audit, on the other hand, has carried itself with decorum and integrity. My poem attempts to reflect this.

Saviour Internal Audit

Atheoretical, indeterminate, inscrutable, malleable,
Wobbly jelly at least has basic shape,
This undivine mystery disappears into gaseous nothingness,
Contradicting chemical axiom of conservation of matter,
Untouched by significant philosophical mind,
Wrestled over by academic and regulator,
Pragmatic practitioner flays out in uncertain certainty,
The quick buck syndrome, capitalistic support,
Abjure the public interest, excepting in professional proclamation.
What is this formless insidious bubble?
A bubble so expansive as to bring the world to its knees,
Did we learn nought from the South Seas Bubble species centuries back?
How is Century 21 unsophisticated bumbling along on bubbles?
I'm forever blowing bubbles; transformed from lyric to de facto professional motto.
Financial Reporting is the name, Accounting the profession,
External Auditing the co-conspirator,
Global industry, huge employee numbers, cost and spawned secondary income,
Frenetic worldwide activity, from Abacus to high information technology,
Heads down quill penning to heads level computer PC,
Yet elusive conceptual frameworks pander fraud and misreporting,
Mindless expansive materiality the shifting sands of million dollar misstatement,
Truth and fairness the disguise for a multitude of sins,

Argue over principles-based versus legal based,
Argue over professional discretion and flexibility,
Open the floodgate to the unscrupulous,
Balance sheets and balanced scorecards,
Where was the balance in Enronitis and its ignoble antecedents and successors?
UK hide behind Caparo,
Public can only dream judges will extend this limiting judgement,
Recognise stakeholding beyond current shareholding,
Uphold wider interests, as one by one the succession of assumed controls erode.
Expectations gap expanded to chasm gap,
As innocent public and employees count the cost,
At least they have accurate view of cost,
Being devoid of accountants, auditors and financial reporting standards.
Their cost is unemployment, loss of pension, arbitrary loss of quality of life.
They can count, how cannot the putative professionals count?
Their real-time reporting is in the weekly grocery bill,
Gross time-lapse financial reporting risks all.
The subtlety of internal controls without internal control,
Pick at the minutiae and miss the totality,
Concentrate on the Biblical mote and unobserve the beam,
Internal audit in quandary:
Follow external audit into the abyss,
Or speak out, be counted, and maybe dismissed,
Or become the unsung hero, occasionally seeing the light of day and public acclaim.
Those in the know may whistleblow,
Casting their career on choppy waters,
Protected yet sacrificial unprotected,
Uphold professional dictate,
Often enjoying derisory professional support,
Not even a press release to mark their demise and discomfort.
Vindication fortuitous.
Should the reporting system rely on whistleblower?
The best synergy of theory and practice?
The chance event of stimulus and response,
The one in a million whistleblower prepared to take on the system,
Unassisted by financial reporting convention and audit practice.
Corporate governance the solution?
Myriad reports, blue ribbons, senate hearings, state audit reports,
still seepage of shareholder and stakeholder wealth.
Company law revision the prelude to revision of capitalistic attitudes.
The challenge to prove anti-capitalist protesters wrong,
otherwise they alone represent disruptive sanity,
the last cry of the desperate to reform the insupportable,
obvious to all, but the world turns irrespective,
crushing the vulnerable as well as the average citizen.
Change of heart and attitude more difficult than formal reform.
All hands to the tiller for a concerted and focused attempt to stem abuse,
professionals, directors, auditors, accountants, lawyers, employees and more unite,

the task formidable,
the task neglected,
the consequences cataclysmic.
Let history look back and recognise this was the generation which acted,
the generation which side-stepped complacency,
extinguished expectations gaps perpetrated by all former professional partners-in-crime.
Internal audit with unsullied reputation and hence unrivalled opportunity,
The golden wonder child of corporate governance report,
Ride into the affray,
Marshal the contending parties,
Risk manage advise,
Dynamically unite all to the common purposes:
Bolster organizational performance, economies and public welfare.

The late Professor Gerald Vinten
European Business School London
Chartered Institute of Public Finance and Accountancy
Former editor, *Managerial Auditing Journal*

Appendix D

ANALYTICAL TECHNIQUES BY SUE SEAMOUR

Analytical techniques (also called analytical procedures) are the comparative analysis of figures against expected trends or previous results and the study of relationships between data and information from different sources. External auditors use them to help form an opinion on the accuracy of published accounts. However, they are also useful tools for internal auditors.

They can be used when the internal auditor is learning about the system to be audited and during testing. For ease they can be divided into three types:

1. Ratio analysis
2. Proportional analysis
3. Trend analysis

They are almost invariably used in combination.

Ratio Analysis

These are used on accounting and financial data to:

- Predict future trends to assist in planning audit strategy.
- Identify indications of problems.

Examples of key ratios include:

Gross profit %	$\frac{\text{gross profit}}{\text{sales}} \times 100$
Liquidity	$\frac{\text{current assets}}{\text{current liabilities}}$
Debtors ratio (number of days' sales in debtors)	$\frac{\text{debtors}}{\text{sales}} \times 365$

They are meaningful only if compared to other data such as previous periods, industry indicators, targets (e.g. liquidity ratio set as loan condition).

Proportional Analysis

Includes, e.g.:

- Number of employees against total payroll bill.
- Bank interest as a % of bank balances.

- Dividend returns against market averages.
- Power charges against industry tariffs.
- Overtime as a percentage of gross pay.

Trend Analysis

Includes comparison with:

- Historical experience.
- Industry average/norms.
- Budgets.
- Past performance analysis.
- Inter-unit/region/division comparisons.
  - Requires identification of unexpected, extreme or unusual results and variances from targets.
  - Trends can be based on seasonal, cyclical or other mathematical analysis such as regression analysis.

Examples of the Use of Analytical Techniques

1. Sales: Examine the pattern of sales over past periods and review seasonal levels. Review the sales mix in relation to product changes and market conditions. Calculate ratios of cost of sales, staff numbers, overhead costs. It may be possible to examine ratios for the same operation within other parts of the organization, or within other organizations.

2. Stores system: Review the mix of stores items by value. Examine the pattern of purchases over past periods for types, amounts and suppliers in relation to products and sales. Review the pattern of stores issues over past periods. Calculate the rates of item usage. It may be possible to examine ratios for the operation within other parts of the organization, or within other organizations.

3. Cash and banking system: Review changes in cash and bank balances during the period in conjunction with other relevant information, sales and debtors, and capital expenditure. Compare actual cash flows with budgets, analyse variances and establish the reasons for them. If the information is available examine ratios for the same operation within the organization or within other organizations.

4. Payments system: Examine the pattern of payments over periods and review seasonal levels. Review the mix in relation to purchase patterns, contracts, sales and product changes. Calculate number of days between date of payment of invoice with previous periods, policy and industry norm. Calculate ratios of payments to sales and purchases. Compare with same operation internally and, if possible, with other organizations.

Using the Results

The results of analytical techniques can be used to:

- Gain a better understanding of the system/area.
- Provide assurance on the operation of the system if the expected relationship is found to exist.

- Indicate areas for further audit work where the expected relationship is not found or there are significant variations between areas/organizations.
- Direct management's attention to unusual variations.

An Example of Analytical Techniques Turning Data into Information

In isolation, a number is not very useful. For example, when auditing human resources to say that the total full-time equivalent staff in post in 2003/2004 was 1,402 is not very illuminating. We begin to get an understanding if we look at this together with other numbers. We can look at trends, comparisons and ratios. We can also look at a more specialized form of trends, i.e. indexing.

Trends We can establish more about what is happening if we look at the staff in post over a period of time. From the figures below, we can see there is a growth in the number of staff. Without more information we don't know whether this warrants our interest.

Staff in post	**99/00**	**00/01**	**01/02**	**02/03**	**03/04**
Area 4	1,310	1,340	1,367	1,385	1,402

Comparisons The figures below show the trends for all areas. We can see that while Areas 2 and 4's staffing was growing, Area 3's was shrinking and Area 1's was fluctuating. This gives us questions to ask about what was happening in the different areas and where the differences spring from. There could be differences in the workloads or better control in some areas.

Staff in post	**99/00**	**00/01**	**01/02**	**02/03**	**03/04**
Area 1	382	390	276	350	391
Area 2	1,161	1,189	1,257	1,298	1,322
Area 3	1,611	1,601	1,518	1,510	1,485
Area 4	1,310	1,340	1,367	1,385	1,402

Ratios If we look at the staffing in relation to turnover, i.e. how much money is taken by the operation, we can ask still more questions. Why is there such a difference between the figures for Area 2 and Area 4? Why is Area 4 static while Area 2 is falling?

Staff in post	**99/00**	**00/01**	**01/02**	**02/03**	**03/04**
	£000	£000	£000	£000	£000
Area 1	16.3	16.2	16.8	16.9	17.1
Area 2	15.8	15.9	15.8	14.9	14.7
Area 3	17.1	17.2	17.2	17.8	18.5
Area 4	18.9	18.4	18.3	18.6	18.6

Indexing Trends stand out even more clearly if we express figures as a percentage of the first year.

Staff in post	**99/00**	**00/01**	**01/02**	**02/03**	**03/04**
Area 1	100	102	72	92	102
Area 2	100	102	108	112	114
Area 3	100	99	94	94	92
Area 4	100	102	104	105	107

Using analytical techniques has become even easier now that so much data and information are held on computers. Many information systems have powerful ad-hoc reporting facilities that allow the auditor to analyse data in a myriad different ways. The spreadsheet package on your desktop or laptop will also readily allow you to use these techniques.

At one time internal auditors mainly used analytical techniques as part of formal interrogation packages (i.e. as a computer assisted audit technique). We now recognize their usefulness as a tool, both formal and informal, that deepens our understanding of the activities we are auditing and gives us a ready means of identifying areas for further audit work.

Appendix E

MULTI-CHOICE QUESTIONS: ANSWER GUIDE

Chapter 1: Multi-choice Questions

1.1. (Answer d)
1.2. (Answer a)
1.3. (Answer e)
1.4. (Answer b)
1.5. (Answer a)
1.6. (Answer b)
1.7. (Answer d)

Chapter 2: Multi-choice Questions

2.1. (Answer b)
2.2. (Answer d)
2.3. (Answer d)
2.4. (Answer b)
2.5. (Answer a)
2.6. (Answer c)
2.7. (Answer b)
2.8. (Answer c)
2.9. (Answer f)
2.10. (Answer d)
2.11. (Answer b)
2.12. (Answer b)
2.13. (Answer d)
2.14. (Answer b)
2.15. (Answer c)
2.16. (Answer c and f)
2.17. (Answer b)
2.18. (Answer c)
2.19. (Answer b)
2.20. (Answer a)
2.21. (Answer c and g)
2.22. (Answer d)
2.23. (Answer b)
2.24. (Answer d)

2.25. (Answer d)
2.26. (Answer b)
2.27. (Answer c)
2.28. (Answer a)
2.29. (Answer d)
2.30. (Answer c)
2.31. (Answer a)

Chapter 3: Multi-choice Questions

3.1. (Answer b)
3.2. (Answer d)
3.3. (Answer a)
3.4. (Answer c)
3.5. (Answer b)
3.6. (Answer b)
3.7. (Answer a)
3.8. (Answer c)
3.9. (Answer – Risk registers)
3.10. (Answer d)
3.11. (Answer b)
3.12. (Answer a)
3.13. (Answer e)
3.14. (Answer c)
3.15. (Answer (b) should be informational)
3.16. (Answer c)
3.17. (Answer d)
3.18. (Answer b)
3.19. (Answer c)
3.20. (Answer d)
3.21. (Answer b)
3.22. (Answer a)

Chapter 4: Multi-choice Questions

4.1. (Answer c)
4.2. (Answer a)
4.3. (Answer a)
4.4. (Answer c)
4.5. (Answer c)
4.6. (Answer d)
4.7. (Answer b)
4.8. (Answer c)
4.9. (Answer a)
4.10. (Answer d)
4.11. (Answer a)
4.12. (Answer d)

4.13. (Answer b)
4.14. (Answer e)
4.15. Answers below:
   a. Purpose
   b. Commitment
   c. Capability
   d. Action
   e. Monitoring and learning
4.16. (Answer a)
4.17. (Answer c)
4.18. Answers below:
   a. Fire alarms. **(Det)**
   b. Staff awareness training where the importance of guarding against fire. **(Dir)**
   c. Fire appliances and fire extinguishes. **(C)**
   d. Banning unauthorized electrical appliances. **(P)**
4.19. (Answer b and f)
4.20. (Answer c)
4.21. (Answer b)
4.22. (Answer 6)
4.23. (Answer c)
4.24. (Answer a)
4.25. (Answer b)
4.26. (Answer d)

Chapter 5: Multi-choice Questions

5.1. (Answer b)
5.2. (Answer a)
5.3. (Answer d)
5.4. (Answers points e, j, l and m)
5.5. (Answer d)
5.6. (Answer b)
5.7. (Answer d)
5.8. (Answer f)
5.9. (Answer b)
5.10. (Answer a)
5.11. Answers below:
   a. The outsider
   b. The manager by proxy
   c. The autonomist
   d. The absolutist
5.12. (Answer c)
5.13. (Answer c)
5.14. (Answer b)
5.15. (Answer d)
5.16. (Answer b)
5.17. (Answer c)

5.18. (Answer b)
5.19. (Answer e)
5.20. (Answer b)
5.21. (Answer a)
5.22. (Answer correct order 26, 48, 24, 02%)
5.23. (Answer correct order 11, 58, 23, 08%)
5.24. (Answer d)
5.25. (Answer f)
5.26. Answers below:

Box 1; g
Box 2; a
Box 3; b
Box 4; d
Box 5; e
Box 6; f
Box 7; b
Box 8; h

5.27. (Answers c)
5.28. (Answers b)
5.29. (Answers a)
5.30. (Answers h)
5.31. (Answer a)

Chapter 6: Multi-choice Questions

6.1. (Answer d)
6.2. (Answer b)
6.3. (Answer d)
6.4. (Answer e)
6.5. (Answer b)
6.6. Answers below:

	Assurance	Consulting
a. advice		×
b. compliance	×	
c. counsel		×
d. due diligence	×	
e. facilitation		×
f. financial	×	
g. systems security	×	
h. process design		×
i. training		×

6.7. (Answer b)
6.8. (Answer b)
6.9. (Answer g)

6.10. (Answer a)
6.11. (Answer e)
6.12. (Answer j)
6.13. (Answer d)
6.14. (Answer a)
6.15. Answers below:

Concepts	Descriptions a, b, c or d
1	b
2	a
3	d
4	c

6.16. (Answer b)
6.17. (Answer a)
6.18. (Answer d)

Chapter 7: Multi-choice Questions

7.1. (Answer b)
7.2. (Answer c)
7.3. (Answer d)
7.4. (Answer a)
7.5. (Answer b)
7.6. (Answer d)
7.7. Answers below:

Systems concepts:	Description a, b, c, d or e
Managerial, operational and functional	d
Parent system, main systems and sub-systems	b
Subjective system	a
Systematic	c
Systemic	e

7.8. (Answer b)
7.9. (Answer a)
7.10. Answers below:

a. Follow company vehicles to see whether they were being used on official business.

SBA or TBA
×

b. Observe several vehicles during the course of the audit to check the way these controls are operating

SBA or TBA
×

c. Isolate and review controls over the process of preparing invoices and paying suppliers.

SBA or TBA
×

d. Examines a sample of payments to see if they are correct and proper without commenting on the underlying controls.

SBA or TBA
×

7.11. (Answer d)
7.12. (Answers c, i and n)
7.13. (Answer a)
7.14. (Answer c)
7.15. Answers below:

Types	Description a, b, c or d
1. Process	d
2. Projects	b
3. People	c
4. Preparedness	a

7.16. (Answer b)
7.17. (Answer e)
7.18. Answers below:

Style	Description a–d
Activist	c
Reflectors	d
Theorists	b
Pragmatist	a

7.19. (Answer d)
7.20. (Answer c)
7.21. (Answer a)
7.22. (Answer b)
7.23. (Answer b)
7.24. (Answer a)
7.25. (Answer c)
7.26. (Answer a)
7.27. (Answer a)
7.28. (Answers j and n)
7.29. Answers below:

1. Clarity
2. Indexed
3. Support the audit decisions/opinion
4. Defend conclusions
5. The use of pro formas
6. Cross referenced
7. Economically used
8. Headed up
9. Clearly shows the impact on the investigation
10. Signed by the officer and the reviewer
11. Show the work carried out
12. Set out the objectives of the work
13. Indicate which matters are outstanding

14. Dated
15. Show any impact on the next stage of the investigation
16. Complete
17. Set out in a neat and orderly fashion
18. Consistent
19. Simple
20. Required
21. Includes summaries
22. Reviewed
23. Shows the source of information/data
24. Logically arranged

7.30. (Answer e)
7.31. (Answers d and g)
7.32. (Answers e, h and j)
7.33. (Answer b)
7.34. (Answer e)
7.35. (Answer g)
7.36. Answers below:

Type	Description (a, b or c)
1. Cold stand-by centres	b
2. Warm stand-by centres	a
3. Hot stand-by centres	c

7.37. (Answer c)
7.38. Answers below:

1. access, security and passwords control (IC)
2. All expected output is received (OC)
3. an adequate transaction trail should be available so that data may be traced to the original or and through the system (OC)
4. anti-virus software (IC)
5. appropriate format (OC)
6. authorization (IC)
7. batch control (where appropriate) (IC)
8. call back for remote access (IC)
9. check digits (PC)
10. checkpointing – saving transactions at a certain point in time (PC)
11. compatibility checks – consistent field used (PC)
12. completeness checks, e.g. all fields covered and all data is accounted for (PC)
13. completeness, e.g. batch numbers (IC)
14. completeness schedules of expected output (OC)
15. control totals (IC)
16. control totals (PC)
17. controlled stationary (IC)
18. data is quickly re-submitted wherever necessary (OC)
19. disciplinary with instant removals of staff (IC)
20. disposal or documents and reports (OC)
21. double keying and verification (IC)
22. duplicate input checks (PC)

23. encryption (IC)
24. error messages (IC)
25. error reports (OC)
26. e-transfers authorized (IC)
27. exception checks – e.g. overtime only given to certain grades of officers (PC)
28. exception reports (OC)
29. exception reports (PC)
30. exceptions are investigated by a responsible officer (OC)
31. file identification controls (PC)
32. firewalls and authentication routines (IC)
33. format checks – that ensure the item is either alpha or numeric (PC)
34. good security arrangements for reports in line with Data Protection rules (OC)
35. independent check on all output (OC)
36. limit checks (PC)
37. logical routines (PC)
38. manual procedures to ensure all reports reach their destination (OC)
39. mechanisms to ensure that the output is received in a timely fashion (OC)
40. missing data checks (PC)
41. overflow flags that indicate where excess digits have been used (PC)
42. page numbering (OC)
43. physical access restrictions (IC)
44. prioritization of output (OC)
45. range checks – so that a transaction must be between say £0 and £20,000 (PC)
46. reconciliation of related fields (PC)
47. record count (PC)
48. recovery procedure (PC)
49. reference documents (OC)
50. reports only sent to authorized users (OC)
51. rules on automated document retention and storage (OC)
52. run to run controls – e.g. total gross pay from the Gross Pay programme should be the input to the Net Pay programme (PC)
53. screen viewing restricted to authorized personnel (OC)
54. secure printers (OC)
55. security over valuable stationery (OC)
56. segregation of duties (IC)
57. sequence checks on consecutive numbering (PC)
58. sequential numbers (IC)
59. shredders for confidential waste (OC)
60. staff training and recruitment (IC)
61. suitable reports (OC)
62. supervisors review and authorization (IC)
63. systems failure controls (PC)
64. the appropriate media used (OC)
65. the whole validation programme (PC)
66. turnaround documents (IC)
67. user feedback to ensure that reports are no longer sent where they are not used (OC)

68. user procedures (IC)
69. validation – range, format, reasonableness (IC)
70. validation (display data after routine) accuracy checks (IC)
71. validity checks – say checking that a correct code has been used (PC)
72. well designed input documents (IC)
73. well planned error and exception reports (OC)
74. working documents (OC)

7.39. (Answer a)
7.40. (Answer 4, f)
7.41. Answers below:

Economy: Resources required to perform the operation are acquired the most cost-effectively.

Efficiency: Resources are employed to maximize the resulting level of output.

Effectiveness: Final output represents the product that the operation was set up to produce.

7.42. Answers below:
a. efficiency
b. efficiency
c. economy
d. efficiency

7.43. (Answer d)
7.44. (Answer b)
7.45. (Answer h)
7.46. (Answer c)
7.47. (Answer b)
7.48. (Answer d)
7.49. Answers below:
a. A genuine fear of change can add to this resistance. (R)
b. Better materials can lead to faster and leaner production. (D)
c. Competition forces change and is perhaps the single most important driving factor. (D)
d. Complacency is a real dampener. The 'two years to retirement' syndrome is not conducive to any real change as a key manager seeks a containment position until he/she retires. (R)
e. Group norms for group performance that restrict the push for change. (R)
f. New IT and better systems create an almost unlimited scope to spot and develop change routines. (D)
g. Supervisors' pressures for better performance in line with a suitable strategic direction. (D)
h. Well-learned skills that may become redundant and this may fall on the wrong side of the individual cost benefit equation. (R)

7.50. (Answer f)

Chapter 8: Multi-choice Questions

8.1. (Answer c)
8.2. (Answer d)

8.3. (Answer a)
8.4. (Answer i)
8.5. (Answer a)
8.6. (Answer c)
8.7. (Answer e)
8.8. (Answer c)
8.9. (Answer b)
8.10. Answers below:
   a. conceptualizing skills
   b. communicating skills
   c. technical skills
8.11. (Answer c)
8.12. (Answer a)
8.13. (Answer d)
8.14. (Answer f)
8.15. (Answer d)
8.16. (Answer b)
8.17. (Answer f)
8.18. Answers below:
   - November – start the new planning process and build in extra capacity for consulting requests for management (via a formal assessment criteria). (f)
   - December – draft risk assessment forms and review of corporate risk database. One audit team uses the following allocations of productive audit time that is assigned in outline to: 50% annual audit plan, 20% emerging risk issues, 7% special investigations, 20% special projects, 3% follow up. (b)
   - January/February – analyse information and talk to senior management and the board and include agree consulting projects. (a)
   - March – finalize the annual audit plan and send discuss with audit committee. (c)
   - End March – publish the plan and allow update facilities. (e)
   - April – plan now live. (d)
8.19. (Answer d)
8.20. (Answer f)
8.21. (Answer d)
8.22. (Answer a)
8.23. (Answer d)
8.24. (Answer e)
8.25. (Answer b)
8.26. (Answer c)
8.27. (Answer b)
8.28. Answers below:

A–D Headings:

   1. It must play a role in evaluating auditor's performance (D).
   2. The manual has to be used by auditors (C).
   3. The task has to be properly resourced (A).
   4. The wide concept of the manual has to be supported (B).

8.29. (Answers a, e and i)
8.30. (Answer d)
8.31. (Answer a)

8.32. Answers below:

Term	Description (a, b or c)
1. Strategic	b
2. Managerial	a
3. Operational	c

8.33. Answers below:

1. Timeliness
2. Quantity
3. Efficiency
4. Effectiveness
5. Documented
6. Accepted
7. Security catered for
8. Flexible
9. Relevant
10. Accurate

8.34. (Answer b)
8.35. (Answers e and k)
8.36. (Answer c)
8.37. (Answers e, g, k and s)
8.38. (Answer f)
8.39. (Answer e)
8.40. (Answer d)
8.41. (Answer c)
8.42. (Answer b)

Chapter 9: Multi-choice Questions

9.1. (Answer d)
9.2. (Answer a)
9.3. (Answer b)
9.4. (Answer d)
9.5. (Answer c)
9.6. (Answer b)
9.7. (Answer f)
9.8. (Answer c)
9.9. (Answer c)
9.10. Answers below:

Sources of first impressions	Importance on forming an impression
1. Visual impact (what is seen)	55% (b)
2. Auditory impact (what is heard)	38% (a)
3. Content (what is said)	7% (c)

9.11. (Answer a)
9.12. (Answer e)

9.13. (Answer b)
9.14. (Answer d)
9.15. (Answer e)
9.16. Answers:

Question type:	Example (a–h)
1. Open questions	d
2. Closed questions	a
3. Probing questions	e
4. Confirmatory questions	h
5. Clarification	b
6. Leading questions	c
7. Loaded questions	f
8. Trick questions	g

9.17. (Answers g and l)
9.18. (Answer a)
9.19. (Answers c and e)
9.20. (Answer b)
9.21. (Answer g)
9.22. Answers below:
a. document
b. book
c. computer process
d. control
e. computer printout
f. ghosting
g. operation
h. connector
i. computer disc
j. file
k. pre-numbered document
l. alternative process
9.23. Answers below:

Narrative:	Description (a, b, c or d):
1.	d
2.	a
3.	c
4.	b

9.24. (Answer e)
9.25. (Answer b)
9.26. (Answer g)
9.27. (Answer c)
9.28. (Answer, advantage 8, disadvantage 3)
9.29. (Answer d)
9.30. (Answer g)
9.31. (Answer b)
9.32. (Answer d)

9.33. Answers below:

Test type	Description (1, 2, 3 or 4)
A.	3
B.	2
C.	1
D.	4

9.34. Answers below:

Box	Description (1, 2, 3 or 4)
A.	2
B.	4
C.	1
D.	3

9.35. (Answer e)
9.36. (Answer d)
9.37. (Answer a)
9.38. (Answer i)
9.39. (Answer c)
9.40. (Answer b)
9.41. (Answer d)
9.42. (Answer a)
9.43. (Answer c)
9.44. (Answer b)
9.45. (Answer a)
9.46. Answers below:

Attribute:	Description (a, b, c or d):
1. Sufficient.	d
2. Reliable.	b
3. Relevant.	c
4. Practical.	a

9.47. (Answer q)
9.48. Answers below:

1. Audit review notes. (C)
2. Budgets and other financial data. (P)
3. Board papers. (P)
4. Any audit programme used. (C)
5. Corporate and operational system notes. (P)
6. Corporate Risk Register. (P)
7. Internal Control Evaluation Schedules. (C)
8. Management reports. (P)
9. Systems notes and flowcharts. (C)
10. The assignment plan. (C)
11. The system evaluation. (C)
12. Organization charts. (P)
13. The audit report. (C)
14. Previous audit reports. (P)

15. Research items and relevant publications. (P)
16. The objectives statement. (C)
17. Summaries of frauds. (P)
18. The preliminary survey and risk assessment (risk registers). (C)
19. The results of any background research carried out. (C)
20. List of premises and addresses. (P)
21. The scope of the audit. (C)
22. The test results. (C)
23. The testing strategy. (C)

9.49. (Answer d)
9.50. (Answer e)
9.51. Answers below:

Types of sampling:	Description:
1. Judgement sampling.	b
2. Indiscriminate sampling.	c
3. Statistical sampling.	a

9.52. Answers below:

Type of sampling:	Description:
Random sampling.	e
Stratified sampling.	b
Cluster sampling.	d
Interval sampling.	c
Automated sampling.	a

9.53. Answers below:

Statistical term:	Description (a, b, c or d):
1. Error rate	b
2. Confidence	a
3. Precision	d
4. Extrapolation	c

9.54. Answers below:

Plan:	Compliance test (C) or Substantive test (S):
Attribute sampling	(C)
Difference estimates	(S)
Discovery sampling	(C)
Monetary unit sampling	(S)
Stop-go sampling	(C)
Variable sampling	(S)

9.55. (Answer c)
9.56. (Answer e)
9.57. (Answer a)
9.58. (Answer d)
9.59. (Answer c)
9.60. (Answer a)
9.61. (Answer a)

9.62. Answers below:

Jargon	Preferred
1. due to the fact that	b
2. endeavour	k
3. evaluate	j
4. expeditiously	i
5. facilitate	g
6. finalize	e
7. for a period of	f
8. for the reason that	c
9. generate	h
10. have been shown to be	a
11. implement	d

9.63. (Answer c)
9.64. (Answers f and g)
9.65. (Answer b)
9.66. (Answer e)
9.67. (Answer f)
9.68. (Answer a)
9.69. (Answer j)
9.70. (Answer b)
9.71. (Answers f and j)
9.72. (Answer a)
9.73. (Answer h)
9.74. (Answer d)
9.75. (Answers b, k and p)
9.76. (Answer c)
9.77. (Answer b)
9.78. Answers below:

Term:	Description:
1. Criteria	d
2. Condition	a
3. Cause	b
4. Effect	c

9.79. (Answer f)
9.80. (Answer f)
9.81. (Answer d)
9.82. (Answers b, d, h, k and n)
9.83. (Answer a)
9.84. (Answer d)
9.85. (Answers b and c)

Chapter 10: Mulit-choice Questions

10.1. (Answer b)
10.2. (Answer d)

INDEX

Accountability, audit and, 57
  audit committee and auditors, 57
  financial reporting, 57
  internal control, 57
Accountability systems, 644
Accounting staff, 372
Accounts, auditing controls versus, 92
Accurate communications, 442
Advance Disclosure of Evidence Act, 578
Advertizing standards, 650
Alder Hey Hospital, 44–45
Alleged system, 864–865
Allfirst, 46
Allied Irish Bank (AIB), 46
Analytical techniques by Sue Seamour, 1037–1040
  proportional analysis, 1037
  ratio analysis, 1037
  trend analysis, 1037
Annual audit plan, 795
Annual audit reports, 921
Annual reporting cycle, 961–964
  audit environment, 962
  input, 962
  output, 962
  process, 962
  recipients, 961
Anti-fraud program, 712
Anti-Terrorism, Crime and Security Act, 35
Anxiety in formal presentation, 953–955
  breathing, 954
  eye contact with the audience, 954
  good presentation, 953
  muscle tension, 954
  poor presentation, 953
  practice makes perfect, 954
  preparation is the key to success, 954
Application auditing, 631–632
  input controls, 632
  output controls, 632
  processing controls, 632
Appraisal process, 722
Ascertaining the system, 858–864
  alternative methods, 858
    block diagrams, 858, 860
    flowcharts, 858, 860–861
    internal control questionnaire (ICQ), 858
    narrative notes, 858–860
  balancing the level of details required, 863–864
  Rutteman, 861–862
Aspirational model, 360
Assessment services, 654
Assignment planning, in audit planning, 832–836
  assignment planning process, 835
  planning documentation, 835–836
  time budgets, 834–836
Association of Insurance and Risk Managers (AIRMIC), 190
Assurance, Control and Risk (ACR), 449
Attribute sampling, 918
Audit 21, 106–107
Audit approach, 505–676
  compliance, 636–642
  consulting approach, 653–669
    assignment sequences, 654–655
    change management, 658–659
    change strategy, 665–666
    force-field analysis, 663–665
    implications of change, 660–661
    individual cost–benefit analysis, 661
    investigations, performing, 655–658
    need for change, 659–660
    resistance to change, 661–663
    stress, dealing with, 666
    types, 654
  contract audit, 652–653
  control risk self-assessment (CRSA), 523–531
  facilitation skills, 531–539
    good facilitator, skills of, 532–534
    group behaviour, 536–539
    learning styles, 534–535
    tools, 537–539
  factors impacting, 506
    main requirements, 507
  financial audits, 650–652
  fraud investigations, 543–586
  information systems auditing, 586–636
  new developments, 675–676
  right structure, 669–675
    centralized audit department, 669
    client-based groups, 669
    consultancy-based models, 670
    decentralized departments, 669
    hierarchical structures, 670
    individual work, 671–672
    influencing factors, 670
    minimum numbers, 674
    mixed structures, 669
    project teaming, 670
    project teams, 672–673
    project-based approach, 670
    service based, 673
    service-based functions, 669
    status of internal audit, 671
    supervisors, 674–675
    trainees, 675
  self-assessment, integrating with, 539–543
    background research and presentation, 542
    Canada Life, 540–543

Audit approach (*continued*)
CSA workshop with staff, 542
key risk and control matrix production, 542
report production, 543
test key controls, 542–543
social audits, 647–650
systems approach, 506–522
affected by being in a system, 508
Andy Wynne on Systems, 518–520
assembly of components, 508
business systems, 520–522
connected components, 508
Entropy, 511–512
general systems thinking, 510–511
key systems issues, 515–516
performance standard 2100, 507
risk-based systems Auditing (RBSA), 513–515
soft systems, 522
systems versus transactions approach, 512
systems, features of, 507–510
systems-based auditing (SBA), benefits, 516–518
transactions approach, 512–513
systems auditing, 505–506, 511
value for money, 642–647
Audit assignment reports, 923–925
executive summaries, 923
follow-up reports, 923
fraud investigation reports, 925
oral reports, 925
staff appraisal reports, 925
Audit brief, 873
Audit budget, 490
Audit charter, 325–334, 773
key issues, 326–330
role of, 325–326
structure, 330–331
Audit clearance procedures, 959
Audit Commission Act 1998, 108
Audit commission, 107–109
fraud, 548
Audit committee reporting, 960–964
annual reporting cycle, 961–964
quarterly reporting cycle, 960–961
Audit committee, 120–136
constitution of, 127–130
development of, 134
DTI review of, 134–135
internal audit perspective, 130–131
NYSE rules, 133–134
public sector (government), 132–133
role of, 122–127
Smith report, 135–136
Audit competencies, 386–393
Competency Framework for Internal Auditors (CFIA), 391–393
continuous professional development, 389–390
Audit cost profile, 490
Audit ethics, 355–363
applicability, 357–360
enforcement, 357–360
principles, 355–357
three-part model, application of, 362–363
underlying models, 360
whistle-blowing, 361–362
Audit feedback questionnaire, 486
Audit field work, 827–1006, *See also* Ascertaining the system; Audit committee reporting; Evidence and working papers; Interviewing skills; Planning the audit; Reporting audit results; Statistical sampling; Testing strategies
developments in, 964–970
Audit manual, 745–757
administrative matters, 749
audit approach and methodology, 748
audit function, managing, 750–751
communicating this to auditors, 746
conceptual framework, applying, 751–752
conceptual model of, building, 749
creativity, impact on, 748
creativity problem, overcoming, 753–755
currency, dynamism, 749–750
defining standards and methods of work, 746
definition, 745
expected standards of performance, measuring, 746
implementing, 756–757
maintaining, 757
management of internal audit, 749
models, selecting, 752–753
operational aspects, 749
procedures, 749
procedures and working paper, 748
role of, 745–747
standardized forms, 747–748
structuring, 755–756
using models, 750
Audit planning process, 789–802
annual audit plan, 790, 795
assess risk priorities, 789
assignment plan, 790
audit, 790
audit of privacy programs, scoping out, 799
audit strategic plan, 790
management controls, 801
operational controls, 801
organizational objectives, 789
outline objectives statement, 790
preliminary survey, 790
priorities, 796–798
quarterly audit plan, 790, 796
reporting process, 790
resource-prioritized areas, 790
resource problems, 798–799
risk profile, 793–795
strategy versus resources, 792–793
technical controls, 801
Audit professionalism, 421
application to smaller organizations, 423–424
contribution of IIA, 425–426
hallmarks of, 426–428
internal auditing standards, 429–453
national health service experience, 424–425
universality of standards, 422–423
Audit relationships, 367–368
internal audit liaison, 368
transaction analysis, 368
Audit reputation, 1010–1012

Audit services, 334–339
types of, 700
Audit snoop, 370
Audit standards, 773–774
Audit strategy, 697–825, *See also* Managing performance; Resourcing audit strategy; Risk-based strategic planning
defining, 701–702
establishing, 702
features of, 706–710
implementation, 710–711
new developments, 802–807
problems, dealing with, 737–745
Audit testing, 630
Audit website, 486–487
Audit work, delegating, 758–761
Auditing controls, versus accounts, 92
Auditing Practices Board (APB) statement, 95–98
Auditor appraisal scheme, implementing factors, 724–726
Auditor's code
accountability, 98
association, 99
clear communication, 99
competence, 99
independence, 98
integrity, 98
judgement, 99
objectivity, 98
providing value, 99
rigour, 99
Auditor's preferred system, 865
Auditors' business cards, 487
Australia, 68–70
Australian ASX Corporate Governance Council, 69
Australian/New Zealand standards on risk management (AS/NZS4360:1999), 206
categories of risk, 209
Automated sampling, 915

Bank of Credit and Commerce International (BCCI), 41
Barlow Clowes, 40
Basle Committee on Banking Supervision, 137–139, 251, 269–271
principles, 270–271
BBC Worldwide, 77–78
Behavioural aspects of interviewing, 845–846
Best system, 866
Block diagrams, 858, 860
Blue Ribbon committee, 120–121
Board, 82
IIA definition, 78
Board Guidance, 735–736
internal audit function, 735
resources, 735
review, 735
Boston box, 485
'Box ticking' approach, 1011
Bribe, 36
Bribery, 548
British American Tobacco p.l.c., corporate governance statements of
audit committee, 119
CSR committee framework, 119
internal control, 118
internal control processes, 119–120
review, 120
risk management, 119–120
British Standard, on risk management, 192
Budgetary control, 372
Business advice service control evaluation, 871
Business-continuity program, 712
Business process, 492
Business professionalism, 427
Business systems, 520–522
processes, 520
projects, 520
teams, 520

Cadbury Report, 1992, 48
importance of the board chairman, 85
key concept behind, 54
principles, 50
Californian Public Employees' Retirement System (CalPERS), 64–66
Canada Life, 540–543
Canadian Institute of Chartered Accountants (CICA), 265
Capital contracts, 652
Centralized audit department, 669
Certificated internal auditors, 456
Chairman, 82
Challenges in internal auditing, 1009–1023
audit reputation, 1010–1012
Doomsayer, 1014
Doubters, 1014
Evangelist, 1014
globalization, 1012–1014
meeting the challenge, 1015–1023
new dimensions, 1009–1010
Pragmatists, 1014
Change management, 658–659
poor change management, indicators for, 668–669
Charter Mark, 479
Chartered Institute of Public Finance and Accountancy (CIPFA) standards, 186, 445–449
code of ethics, 446
internal audit, definition of, 446
organisational standards, 447
Chief audit executive (CAE), 1–2, 95
Civil service code, 31–32
Clapham Rail Crash, 210
Clear communications, 442
Client, 469–470
Client-based groups, 669
Cluster sampling, 915
Coexistence, 97
Cold standby centres, 620
Combined Code, 54–60
Committee of Sponsoring Organizations (COSO), 245, 255–264
communication, 261–262
control activities, 261
control environment, 258–260
information, 261–262
monitoring of, 262–264
risk assessment, 260–261

Committee of Sponsoring Organizations of the Treadway Commission (COSO), 53
Common audit methodology, 96
Common body of knowledge (CBOK), 426
Communication, 288
Companies
  accountability, audit and, 57
  directors, 54–5 6
    board, 54–56
    board balance and independence, 55
    chairman, 55
    chief executive, 55
    information and professional development, 56
    performance evaluation, 56
    re-election, 56
  remuneration, 56–57
  shareholders, relations with, 57–58
Competency Framework for Internal Auditors (CFIA), 391–393
  behavioural skills, 391
  benchmarking against, 480
  Cognitive skills, 391
  units of competency, 392
Complaints procedure, 488
Complete communications, 442
Compliance, 636–642
  meaning of, 889–891
  tests, 916, 918
Comptroller and Auditor General (C&AG), 106
Computer Assisted Audit Techniques (CAATs), 629–631, 893–895
  civil cases, 631
  criminal cases, 631
  future of, 895
  problem with, 894–895
  use of, 893–894
Computer auditing, components, 601
Computer interrogation process, 629
Computer Security Institute (CSI), 588
Concise communications, 442
Conducting formal presentations, 957–959
Conducting the presentation, 953
Confederation of British Industry (CBI), 51
Confirmed listed companies, annual reporting requirements, 53–54
Conflict of interest, 341
  IIA definition, 358
Conspiracy, 549
Constructive communications, 442
Consultancy-based models, 670
Consultancy services, 353
Consulting service, 653–669
  assignment sequences, 654–655
  change management, 658–659
  change strategy, 665–666
  force-field analysis, 663–665
  IIA definition, 457
  implications of change, 660–661
  individual cost–benefit analysis, 661
  investigations, performing, 655–658
    audit planning, 656–657
    available options, 657
    causes of problems, determination of, 657
    detailed field work, 657
    discussion with management, 658
    initial terms of reference, 656
    preliminary survey, 656
    report, 658
    suppositions establishment, 656
    test selected options, 658
    work programme, 656–657
  need for change, 659–660
  resistance to change, 661–663
  stress, dealing with, 666
  types, 654
Consumer behaviour, 489
Continuing Professional Development (CPD), 389–390
  stages of, 390
Continuing professional education (CPE), 390
Contract audit, 652–653
  assimilated skills, 653
  capital contracts, 652
  externalized services, 653
  link to purchasing, 653
  revenue contracts, 652–653
Control and risk self-assessment (CRSA), 214
Control breakdown cycle, 375
Control environment, 258–260
  elements of, 258–259
  IIA definition, 258
Control evaluation perspective, 873–876
  audit brief, 873
  'breakdown approach', 874
  common mistakes, 876
  control objective, 875
  expected control, 876
  good practice, 876
  input control objective, 875
  output controls, 875
  processing controls, 875
Control mechanisms, 274–285
  controls in practice, 276–281
  soft controls, 284–285
  suitability of controls, 281–284
  types, 275
    corrective, 275
    detective, 275
    directive, 275
    preventive, 275
Control Objectives for Information and Related Technology (COBIT), 268–269
  component, 269
Control risk self-assessment (CRSA), 523–531
  background to, 526–527
  development approaches, 528–531
  internal audit role, 527
  internal controls and, 523–526
  positive aspects of, 527
  types, 524–525
Control risk self-assessment (CSA), 291
Controlling delegation, 760
Coordination, 97
Corporate governance-based planning, 808–825
Corporate governance perspectives, 23–161
  agency concept, 24–29
  audit committee, 120–136
  corporate ethics and accountability, 29–39

ethical codes, 31–33
ethical reporting, 36–37
ethics implementation, 34
good codes, impact of, 31
international dimension, 34–36
link to values, 33–34
Reith lectures, 30
social responsibility, 39
temptation, 30–31
whistleblowing, 37–38
external audit, 87–120
internal audit, 136–140
internal control, link to, 141–142
internal controls, reporting on, 142–146
international scandals and their impact, 39–47
models, 47–73
new developments, 146–158
principles, 48
putting governance into practice, 73–87
risk management, link to, 141–142
Corporate reporting, 110–113
control environment, 112
non-financial business risks, 112–113
risk identification and review, 112
Corporate risk strategy, 703–704, 790–792
management participation, 703
risk assessment, 703
Corporate Social Responsibility Review (CSR), 37
Corrective control, 286, 296
Corruption, 548
definition, 35
Cosourcing approach, 778–780
advantages, 780
disadvantages, 780
Cost–benefit analysis, 661
Costs, control, 253
Counselling, 726, 730–731
Court of public opinion, 27
Credit Suisse First Boston (CSFB), 47
Criteria of Control (CoCo), 264–267
principles of assessment, 265
CRSA best practice guide, 1029–1032
contribution of CRSA forum, 1031–1032
future of CSA, 1031
CSA, *See* Control risk self-assessment (CSA)
Currency, dynamism, 749–750
Current files, 901–903
any audit programme used, 902
assignment plan, 901–902
audit report, 903
audit review notes, 903
internal control evaluation schedules, 902–903
objectives statement, 901
preliminary survey and risk assessment, 901
results of any background research carried out, 902
scope of the audit, 901
system evaluation, 902
systems notes and flowcharts, 902
test results, 902
testing strategy, 902

Daiwa Bank, 42–43
Data Protection (DP) Act1998, 624–625
data user, 625
disclosure, 625
offences, 625
personal data, 625
processing, 625
Data Protection Act1984, 578
Decentralized departments, 669
Delegation, audit works, 758–761
barriers to, 759–760
delegation process, 758
establishing control over, 760–761
internal audit, 758–759
levels of, 761
Delinquent manager, 377–378
definition, 377
Deloitte & Touche, risk-management cycle, 207
Department of Trade and Industry (DTI), 26, 111
Detective controls, 286, 296
Dey Report, 66–67
Difference estimates, 917
Directed reading, 398
Directed representations, 867
Directive control, 296
Directors
board, 54–56
board balance and independence, 55
chairman, 55
chief executive, 55
information and professional development, 56
performance evaluation, 56
re-election, 56
Disaster coordinator, 621
Disaster planning, 614
Disaster-recovery program, 712
Discovery sampling, 918
Distillers, 40
Doomsayer, 1014
Doubters, 1014
Due professional care, 448, 453–457
Duty of care, 210
Dynamic audit planning, 808–825
corporate governance-based planning, 808–825
risk-based planning, 809–810
traditional audit planning, 808

E-commerce, 210
Educational model, 360
Effectiveness reviews, 643
Efficiency reviews, 643
Electronic Communications Act 2000, 549
Emergency services, 654
Emergency/contingency system, 865
Emotional states (role playing), 368–369
games, 369
pastimes, 368–369
ritualistic, 368
withdrawal, 368
work activity, 369
Enron, 45
Enterprise risk-management program, 711
Enterprise-wide risk management (ERM), 203–213
government experience, 205
integrating risks, 206–208
key developments, 210–214

Enterprise-wide risk management (ERM) (*continued*)
risk categories, 208–210
activity, 209
assets, 209
continuity of operations, 209
external, 209
financial, 209
HR, 209
information technology, 209
market, 209
operational, 209
people, 209
regulatory, 209
reputation, 209
strategic, 209
targets, 209
Entropy, 254, 511
Equitable Life, 44
Ernst and Young, components of effective risk management, 207
Ethical codes, 31–33
civil service code, 31–32
National Health Service(NHS), 32–33
Nolan principles, 33
Ethical reporting, 36–37
European Foundation Quality Model (EFQM), 480–481
levels of recognition, 481
Evaluation, 864–876
control evaluation, 873–876
as a continuous process, 870–873
defining the system, 864–866
directed representations, 867
flowcharts, 866
internal control evaluation system (ICES), 867, 869–870
internal control questionnaires (ICQs), 867–869
transactions testing, 867
Evangelist, 1014
Evidence and working papers, 896–909, *See also* Current files; Permanent files; Working papers
access to working papers, 908–909
automation, 908
common mistakes, 906
evidence attributes, 896–897
filing systems, 907–908
good practice, 906–909
standardization, 903–904
types of evidence, 897
Examinations, 427–428
Expectations gap, 102, 373–376
External audit
central government, 62–64
corporate governance, 87–120
internal audit, 89–97
External review, 472
Externalized services, 653

Facilitation, 532–539
confronting dimension, 533
feeling dimension, 533
group behaviour, 536–539
individual behaviour, 535
learning styles, 534–535
meaning dimension, 533
planning dimension, 533
services, 654
strategies, 537
structuring dimension, 533
styles, 536
tools, 537–539
valuing dimension, 533
Fad Surfing in the Boardroom, 177
Feedback, 726
client feedback, 730
Financial audits, 650–652
accountability, 651
financial regulations, 651
front line work, 651
information audit, 652
interrogations, 651
Financial regulations, 651
Financial reporting, 57, 102
Financial Reporting Council
combined code, 54–58
Smith report, 135–136
Financial Services Authority's (FSA) Guidance, 38
Flexibility, 293
Flowcharts, 858, 860–861, 866
pros and cons of, 862–863
Force-field analysis, 663–665
driving forces, 664
power audit stages, 664
resisting forces, 664
Forgery, 549
Formal engagement, 654
Formal presentations, 953–959
anxiety, 953–955, *See also* Anxiety in formal presentation
conducting, 953, 957–959
preparation, 953, 955–956
visual aids, 953, 956–957
Fraud, 211, 775
causes, 548
CIPFA categories, 543
components, 547–548
control process, 580–582
control project, 578–579
definition, 545
detection, 551
indicators of, 550–551
investigations, 571–578
investigative process, 561–571
allegation received, 562
background research, 563
barriers definition, 564–565
criminal prosecutions, 569
final completed report, 571
final report, 569
full investigation, 566–567
initial strategy, 565
interim reports, 568–569
internal disciplinaries, 569–571
interviews, 568
investigation plan, 564
managerial support, 564
ongoing review and discussions, 567–568
preliminary report, 563–564

surveillance, 565–566
validation, 562–563
preventive techniques, 579–580
risk areas, 545
roles definition in an organization, 551–555
types, 548–550
Front line work, 651

Gap, allowing for growth, 293
General systems thinking, 510–511
functional, 511
main system, 510
managerial, 511
operational, 511
parent system, 510
subjective system, 510
subsystem, 510
systematic, 510
systemic, 510
GlaxoSmithKline, 75–76
Globalization, 1012–1014
Government internal auditing standards, 449–451
operational standards, 450–451
organisational standards, 450
Great Western Trains, 210
Green movement, 648
Groups, life cycle of, 536
Guinness, 40

'The Hammer', 42
Haphazard sampling, 912
HAS, governance statement of
accountability and audit, 116
board, 115
board members' remuneration, 115
communication with stakeholders, 116–118
interest in shares and debentures, 116
notice and declaration of directorships, 116
Herald of Free Enterprise, 210
Hierarchical structures, 670
HM Treasury, 132
benefits, 99
co-operation, 100
measures, 99
risk appetite, 188
risk management, 180
strategic risk management, 205
Hot standby centres, 620
Human resource management cycle, 715

Idea, 630
Ideal system, 865
IIA, *See* Institute of Internal Auditors (IIA)
Impairment, IIA definition, 358
Impartiality, 342
Independence, 340–355
consultancy branch, reconciling the, 352–355
Courtemanche on, 347–348
director of finance, managing the, 351–352
factors affecting, 344–346
interpretation, 340–341
meaning of, 341–344
professionalism, 351
Rittenberg model, 348
three-component model, 346–347
working model, 348–351
Induction/orientation programme, 1027–1028
Informal engagement, 654
Information systems (IS) auditing, 586–636, 775
application auditing, 631–632
auditor role, 592–599
computer-assisted audit techniques (CAATs), 629–631
data protection, 624–628
disaster coordinator, 621
disaster planning, 614–619
planning, 600–601
resources management, 601
risk, 587–588
security, 610–611
standby facilities, 620
in systems development, 601–607
Information-security program, 712
Information technology (IT), audit, 761–771
development, 762–763
hierarchical structure, 766–767
impact of, 761
IS strategy, 767–768
people involvement, 768
resourcing IT, 765–766
as strategic resource, 763–765
time monitoring systems, 769–771
Inland Revenue, 43
Innovation, 293
Institute of Chartered Accountants in England and Wales (ICAEW), 53
risk management, 190–191, 213
Institute of Internal Auditors (IIA) Attribute Standard 1000, 430 (Purpose, Authority, and Responsibility), 3, 325, 430
Institute of Internal Auditors (IIA) Attribute Standard1010, 430
Institute of Internal Auditors (IIA) Attribute Standard 1100 (Independence and Objectivity), 3, 430–431
Institute of Internal Auditors (IIA) Attribute Standard 1110 (Organizational Independence), 340, 431
Institute of Internal Auditors (IIA) Attribute Standard 1111 (Direct Interaction with the Board), 340, 431
Institute of Internal Auditors (IIA) Attribute Standard 1120 (Individual Objectivity), 340, 431
Institute of Internal Auditors (IIA) Attribute Standard 1130 (Impairment to Independence or Objectivity), 431–432
Institute of Internal Auditors (IIA) Attribute Standard 1200 (Proficiency and Due Professional Care), 4, 432–433
Institute of Internal Auditors (IIA) Attribute Standard 1210 (Proficiency), 432
Institute of Internal Auditors (IIA) Attribute Standard 1220 (Due Professional Care), 433
Institute of Internal Auditors (IIA) Attribute Standard 1230 (Continuing Professional Development), 433

Institute of Internal Auditors (IIA) Attribute Standard 1300 (Quality Assurance and Improvement Program), 4, 433, 459
Institute of Internal Auditors (IIA) Attribute standard 1310 (Requirements of the Quality Assurance and Improvement Program), 433, 460
Institute of Internal Auditors (IIA) Attribute Standard 1311 (Internal Assessments), 434, 460
Institute of Internal Auditors (IIA) Attribute Standard 1312 (External Assessments), 434, 460
Institute of Internal Auditors (IIA) Attribute Standard 1320 (Reporting on the Quality Assurance and Improvement Program), 434–435, 460
Institute of Internal Auditors (IIA) Attribute Standard1321, 442
Institute of Internal Auditors (IIA) Attribute Standard 1322 (Disclosure of Nonconformance), 435, 460
Institute of Internal Auditors (IIA) Performance Standard 2000 (Managing the Internal Audit Activity), 4, 435
Institute of Internal Auditors (IIA) Performance Standard 2010 (Planning), 225–226, 435–436
Institute of Internal Auditors (IIA) Performance Standard 2020 (Communication and Approval), 436
Institute of Internal Auditors (IIA) Performance Standard 2030 (Resource Management), 436
Institute of Internal Auditors (IIA) Performance Standard 2040 (Policies and Procedures), 436
Institute of Internal Auditors (IIA) Performance Standard 2050 (Coordination), 437
Institute of Internal Auditors (IIA) Performance Standard 2060 (Reporting to Senior Management and the Board), 437, 512
Institute of Internal Auditors (IIA) Performance Standard 2100 (Nature of Work), 4, 437, 507
Institute of Internal Auditors (IIA) Performance Standard 2110 (Governance), 437
Institute of Internal Auditors (IIA) Performance Standard 2120 (Risk Management), 222, 438
Institute of Internal Auditors (IIA) Performance Standard 2130 (Control), 438–439
Institute of Internal Auditors (IIA) Performance Standard 2200 (Engagement Planning), 4, 439
Institute of Internal Auditors (IIA) Performance Standard 2201 (Planning Considerations), 439
Institute of Internal Auditors (IIA) Performance Standard 2210 (Engagement Objectives), 439–440
Institute of Internal Auditors (IIA) Performance Standard 2220 (Engagement Scope), 440
Institute of Internal Auditors (IIA) Performance Standard 2230 (Engagement Resource Allocation), 440
Institute of Internal Auditors (IIA) Performance Standard 2240 (Engagement Work Program), 440
Institute of Internal Auditors (IIA) Performance Standard 2300 (Performing the Engagement), 4, 440
Institute of Internal Auditors (IIA) Performance Standard 2310 (Identifying Information), 441
Institute of Internal Auditors (IIA) Performance Standard 2320 (Analysis and Evaluation), 441
Institute of Internal Auditors (IIA) Performance Standard 2330 (Documenting Information), 441
Institute of Internal Auditors (IIA) Performance Standard 2340 (Engagement Supervision), 441
Institute of Internal Auditors (IIA) Performance Standard 2400 (Communicating Results), 4, 442
Institute of Internal Auditors (IIA) Performance Standard 2410 (Criteria for Communicating), 442
Institute of Internal Auditors (IIA) Performance Standard 2420 (Quality of Communications), 442
Institute of Internal Auditors (IIA) Performance Standard 2421 (Errors and Omissions), 443
Institute of Internal Auditors (IIA) Performance Standard 2431 (Engagement Disclosure of Nonconformance), 443
Institute of Internal Auditors (IIA) Performance Standard 2440 (Disseminating Results), 443
Institute of Internal Auditors (IIA) Performance Standard 2500 (Monitoring Progress), 4, 444
Institute of Internal Auditors (IIA) Performance Standard 2600 (Resolution of Senior Management's Acceptance of Risks), 4, 444
Institute of Internal Auditors (IIA) Practice Advisory1120–1, 350–351
Institute of Internal Auditors (IIA) Practice Advisory 1130.A2, 349
Institute of Internal Auditors (IIA) Practice Advisory1230–1, 389–390
Institute of Internal Auditors (IIA) Practice Advisory 2130.A1–22, 586
Institute of Internal Auditors (IIA) Practice Advisory 2340–1 (Engagement Supervision), 464
Institute of Internal Auditors (IIA), 313, 429–445
  attribute standards, 430–435
  code of ethics, 444–445
  performance standards, 435–444
  principles of corporate governance, 71–72
  training and development, 400
Institute of Internal Auditors (IIA).UK&Ireland syllabus, 393–394
Institutional shareholders, 58
  governance disclosures, evaluation of, 58
  dialogue with companies, 58
  shareholder voting, 58–60
Integrated governance, 60–61
  definition, 60
  implementation, 60–61
Integration, 98
Internal Assessments, 434
Internal audit, 62, 136–140
  angle, 716–717
  Basle Committee on Banking Supervision, 137–139
  CIPFA, definition by, 446

corporate governance, 88
delegation in, 758–759
external audit
differences with, 91–94
similarities with, 89–91
King report, 139–140
liaison, 368
outsourcing, 782
status of, 671
Turnbull on, 139
Internal audit, long-term goals for, 711
long-term, defining, 713
priorities, 711–713
anti-fraud program, 712
board and executive management service requests, 713
business-continuity program and the disaster-recovery program, 712
compliance and ethics program efforts, 712
enterprise information for decision making, 712
enterprise risk-management program, 711
information-security program efforts, 712
IT function's efforts to meet business needs, 713
overall governance regime, 712
process management, 713
records management, 712
top three most significant business initiatives, 712
Internal audit performance, 734
enhancing, 734
steps to success, 734–735
advanced (Level5), 735
emerging (Level2), 734
established (Level3), 734
introductory (Level1), 734
progressive (Level4), 734
Internal audit role, 311–410
audit charter, 325–334
audit competencies, 386–393
audit ethics, 355–363
audit services, 334–339
definition, 313–319
CIPFA, 316–317
government internal audit manual, 317–319
IIA's, 313–316
expectations management through web design, 382–386
four main elements, 319–320
implications of the wide scope, 320–323
compliance role, 321–322
expertise, 320
information systems, 322
management needs, 323
safeguarding assets, 320–321
specialists, 323
value for money, 322
independence, 340–355
need of, 311
new developments, 403–410
police officer versus consultant, 363–382
proficiency, 387
resourcing the agreed scope, 323–324
scope within different time frames, 323
skills, 387
training and development, 393–403
benefits of training, 394–396
building on existing knowledge, 402
common body of knowledge, 393
IIA role, 399–400
IIA.UK&Ireland syllabus, 393–394
link into development, 402
monitoring training, 400–402
training auditors, 396–399
Internal audit shop, establishing, 771–778
job coding system, 772
main considerations, 773–777
assurance and consulting services, 776
audit charter, 773
audit manual, 776
audit standards, 773–774
budgets, 776
business planning, 775–776
business risk assessment, 774
code of conduct, 774
fraud work, 775
information systems (IS) audit, 775
launch of the new service, 776
recruitment and selection, 774
training, 774
from step zero, 776–777
executive sponsor, 777
internal audit should be internal to the organization, 777–778
investment in tools, techniques, & technology recommended, 778
Internal auditing, development of, 7–19
1940s debate, 15–17
audit function, evolution of, 8–10
influences on the internal audit role, 17–19
moving internal audit out of accountancy, 12–14
role of the statement of responsibility, 14–15
services, 10–12
internal check procedures, 10
management audit, 12
operational audit, 12
probity-based work, 11
risk analysis, 11
risk-based auditing, 12
spot checks, 11
statistical sampling, 10
systems-based approach, 11
transaction-based approach, 10
Internal auditing standards
Assurance, Control and Risk (ACR), 449
Chartered Institute of Public Finance and Accountancy (CIPFA), 445–449
Institute of Internal Auditors (IIA), 429–445
National Health Service (NHS), 451–453
Internal control evaluation system (ICES), 867, 869–870
Internal control, 141–142, 245–301
awareness training, 292–299
Basle Committee on Banking Supervision, 269–271
control framework, 255–267
control mechanisms, 274–285
Control Objectives for Information and Related Technology (COBIT), 268–269

Internal control (*continued*)
costs, 253
CRSA and, 523–526
definition, 256
evaluation, 297
fallacy of perfection, 289–291
integrating controls, 287–289
International Organisation of Supreme Audit Institutions, 267–268
need for, 245–255
New Developments, 299–301
objectives, 254
procedures, importance of, 285–287
appraisal, 287
compliance, 287
development, 286
discipline, 287
induction, 286
outline, 287
review process, 287
training manual, 286–287
training, 287
reporting on, 142–146
risk management, links to, 272–274
Internal control questionnaire (ICQ), 858, 867–869
advantages, 867
disadvantages, 868
Internal review, 470–472
International Organisation of Supreme Audit Institutions, 267–268
International Professional Practices Framework (IPPF), 506
Interrogation software, 630
100% Interrogation theory, 888–889
Interrogations, 651
Interval sampling, 915
Interviewing skills, 839–858, *See also* Non-verbal communication
barriers to good interviews, 852–855
behavioural aspects of interviewing, 845–846
conduct during an interview, 850–851
dealing with difficult people, 855–856
questions, types of, 848–850
recording the interview, 857–858
standardized procedures, 856–857
structuring, 842–845
types, 840–841
Interviews, 568
Investors in People (IiP), 481–483
elements, 481–482
action, 482
commitment, 481–482
evaluation, 482
planning, 482
ISO 9000 Quality Management Systems, 478–479
IT audit guidance, 669
IT Compliance Institute, 669
IT security, 280

Journals, 428
Judgement sampling, 912

Key risk and control matrix (KRCM), 541
King Report, 67–68
internal audit, 139–140
risk, 178
risk appetite, 189
Kings Cross Disaster, 210

Learning styles, 534–535
activists, 535
pragmatists, 535
reflectors, 535
theorists, 535
Leavers, 732–734
customer, 733
financial, 733
internal business process, 733
learning and growth, 733
Liaison, 587
Liberty National Securities, 43
Local Government Act1972, 548
Lyttelton Port Company Limited, 76

M. Matthey, 77
Management consulting, 458
Management controls, 801
Management information systems (MIS), 211–212
Management's responsibilities, 248–250
control, implementation of, 249–250
control maintenance, 250
control updation, 250
need for controls, determination of, 249
suitable controls, design of, 249
Managing performance, 722–737
adopting excellence, 736–737
appraisal criteria, 723–724, *See also* Staff appraisal
auditor appraisal scheme, implementing factors, 724–726
career development, link into, 729
client feedback, 730
counselling, 726, 730–731
feedback, 726
leavers, 732–734
overall productivity, 731–732
performance targets, 724
single audit evaluation, 732
skills levels, 724
training and development, 729–730
Marketing approach, 484
Marketing consultancy services, 377
Marketing information, 488
Marketing mix, 484–485
price, 485
product, 485
promotion, 485
Marketing plans, 488–489
Merrill Lynch, 47
Metropolitan Police, 42
Monetary unit sampling (MUS), 917
Monitoring systems, audit, 769–771
Monthly progress reports, 921–922
Morgan Grenfell, 43
Motor cycle transport system, 510
Mr Five Per Cent, 42

Narrative notes, 858–860
NASA Policy Directive on Internal Management Controls, 289

National Archives of Australia, 76
National Audit Act1983, 106
National Audit Office (NAO), 106–107
  objectives, 106
  risk management in government bodies, 191
National Health Service (NHS), 32–33, 451–453
  external audit, 62–64
  integrated governance, 60–61
  internal audit, 62
  operational standards, 452–453
    audit strategy, 452
    due professional care, 453
    management of audit assignments, 452–453
    quality assurance, 453
    reporting, 453
  organisational standards, 452
    audit committees, 452
    auditors and review bodies, relationships with, 452
    independence, 452
    management, relationships with, 452
    scope, 452
    staffing, training and development, 452
Nationalism, 423
Need to know/have policy, 276
New York Stock Exchange (NYSE), 87
  listing rules, 133–134
Non-executive directors (NED), 49
  legal responsibilities, 80
  responsibilities, 79
  role of, 82
Non-financial business risks, 112–113
  changing business environment, 113
  external shock, 113
  investment decisions, 113
  people development, 113
  safety & security, 112
Non-verbal communication, 846–848
  eye contact, 846
  general body movement, 846
  hand movement and facial expression, 847
  physical position and posture, 847
  silences, 847
  touching, 847

Objective communications, 442
Objectivity, 340, 342
Occupational fraud, 545
One-minute manager, 364, 949–950
Ongoing monitoring, 434
Open system, 509
Operational controls, 801
Operational procedures, 829–830
Organization for Economic Cooperation and Development (OECD), 70–71
Outsourcing approach, 778–789
  Andy Wynne on, 782–785
  audit process and philosophy, 781
  changing nature of audit shop, 788–789
  individual qualities, 781
  internal audit, 782
  organizational relationships, 781
  vulnerability, 787
Overcontrol, 253

Partnering, 98
People, 492
Performance appraisal scheme, 724–726
Performance system, 281
Periodic reviews, 434
Permanent files, 900–901
  budgets and other financial data, 901
  committee papers, 901
  and current files, linking, 903
  list of premises and addresses, 901
  management reports, 900–901
  organization chart, 900
  previous audit reports, 901
  research items and relevant publications, 900
  risk register, 900
  summaries of frauds, 900
  system notes, 900
Personnel policies, importance, 716–717
Perspective, 492
PESTL analysis, 704–705
  economic, 704
  legal, 704
  political, 704
  social, 704
  technology, 704
Piper Alpha, 210
Place, 492
Planned system, 865
Planning the audit, 827–839
  assignment planning, 832–836
  audit programme, 830
  internal audit plan as roadmap, 839
  internal audit with risk assessments, driving, 837
  larger audits, 836–837
  operational procedures, 829–830
  preliminary survey, 828–832
  preliminary survey report, 832
  risk assessments and auditing priorities, 837–838
  systems-based approach versus probity, 831
Police and Criminal Evidence Act, 568
Pollution, 650
Polly Peck International, 40–41
Power audit, stages, 664
Pragmatists, 1014
Pre-event auditing, 602
Preliminary survey reports, 922
Preparation in formal presentation, 955–956
Pre-payment audit checks, 518–519
Prescribed system, 864–866
Prevention of Corruption Act, 548
Preventive controls, 286
Price, 492
PricewaterhouseCoopers (PwC), 41
PRINCE 2 method, 604
Probity audits, 638
Product concept, 484
Production concept, 484
Productivity, 731–732
  acceptable, 732
  implemented, 732
  qualitative, 732
  time budget, 732
  time frame, 732
Professional body, 428

Professional Briefing Note Five, 38
Professionalism, 421–495
audit, 421–453
best value reviews, 475–478
client definition, 469–470
continuous improvement, 491–494
due professional care, 453–457
external review, 472–475
internal review, 470–472
marketing the audit role, 483–491
acid test, revisiting, 483–484
audit budget, 490
audit feedback questionnaire, 486
audit image creation, 491
audit website, 486–487
auditors' business cards, 487
competitors, analysis of, 489
complaints procedure, 488
consumer behaviour, 489
different approaches, 484
marketing information, 488
marketing mix, 484–485
marketing plans, 488–489
published annual report, 491
service level agreements, 490
new developments, 494–495
professional consulting services, 457–459
quality concept, 459–469
appropriate approach, 462–463
appropriate structures, 463
barriers and constraints, 461–462
code of conduct and standards, compliance with, 463
poor products, 461
quality assurance, link into, 466
quality audit staff, development of, 467
quality equation, 460–461
supervision, 464–466
tools and techniques, 478–483
Programme, 638
Project teaming, 670
Project teams, 672–673
resource, 672–673
Promotion, 493
Proportional analysis, 1037
Public Audit Forum (PAF), 109–110
audit process, principles of, 110
service from public auditors, 110
Public Interest Disclosure Act1998, 37

Quality equation, 460
Quality, 459–460
Quarterly audit plan, 796
Quarterly audit reports, 921
Quarterly reporting cycle, 960–961

Random sampling, 914
Ratio analysis, 1037
Recruitment selection, 717–722
career development profile, 722
introduction process, 721
job application shortlisting, 719
job descriptions, 717–718
job specification, 718
panel members, 721
recruitment, 718–719
selection, 719
Regulation of Investigatory Powers Act2000, 549
Regulatory model, 360
Reith lectures, 30
Release management process, 668
Remedial services, 654
Remuneration, 84
level and make-up of, 56–57
procedure, 57
Reporting audit results, 920–952
action plan, formulating, 942
annual audit reports, 921
audit assignment reports, 923–925
audit expertise, 948
change management, 943
clearance process, 942
formulating recommendations, 936–939
formulating the audit opinion, 934–936
good audit reports, 945–947
interim audit reports, 922
internal audit opinion, art of expressing, 950–952
logical presentation, 943–944
monthly progress reports, 921–922
objectives, 930–932
one-minute manager, 949–950
ongoing drafting, 945
performance standards, 929–930
preliminary survey reports, 922
quarterly audit reports, 921
structuring audit report, 944–945
supportive evidence, 942–943
underlying components of action, 933–934
Reporting process, 925–929
agreed action plans, 928
clear audit objectives, 925
clear well-written drafts, 926–927
client kept involved, 926
consultation on the draft, 927
effective review process, 927
final published assignment report, 928–929
good audit work, 925–926
oral presentations, 928
positive wrap-up meeting, 927
preliminary survey and assignment plan, 925
Residual risk, 179–182
Resourcing audit strategy, 714–722, *See also* Recruitment selection
auditors, attributes of, 716
clear personnel policies, importance, 716–717
internal audit angle, 716–717
human resource management cycle, 715
management's role, 714
management, traditional weaknesses in, 714–715
Reuters, 78
Revenue contracts, 652–653
Review process, 939–942
client satisfaction, 941
expression, 940
findings, 939
gaps, 940
house style application, 941
spelling and grammar, 941

structure, 939
terminology used, 941
tone of the report, 940
Reviews, 644
Richard Greenbury Committee, 51–52
Risk and control evaluation (RaCE), 971–972
Risk assessments and auditing priorities, 837–838
Risk-based auditing, 521, 523
Risk-based planning, 809–810
Risk-based service auditing, 517
Risk-based strategic planning, 698–713
audit strategy, defining, 701–702
audit work, scope of, 699–701
corporate risk strategy, 703–704
objectives, 698–699
PESTL analysis, 704–705
SWOT analysis, 704–705
Risk-based Systems Auditing (RBSA), 513–515
stages of, 514
Risk management, 173–236
Australian/New Zealand standards, 206
challenge, 176–178
control self-assessment, 213–217
awareness seminars, 216
general interest, 215
infrastructure build, 216
integration, 216–217
responsible person, 215
risk exercises, 216
rumblings of research, 215
top management interest, 215–216
definition, 175–176
embedded, 218–220
enterprise-wide, 203–213
internal audit role in, 221–230
mitigation through controls, 182–186
better controls, 183
check compliance, 185–186
commission research, 185
communication, 184
contingencies, 184
external reference, 185
maximization, 184
monitoring performance of controls, 182
termination, 183
tolerance, 184–185
transfer of risk, 183
new developments, 230–236
phases, 204–205
residual risk, 179–182
risk appetites, 186–192
risk policy, 192–203
board sponsor, 194–195
chief risk officer, 199–201
content of, 202–203
people buy-in, 195–198
public risk, 198–199
risk registers, 186–192
stages of, 180–181
assessment, 181
identification, 180
management, 181
review, 181
Risk registers, 119, 186–192
Rittenberg model, 348
economic, 348
mental state, 348
organization, 348
Rutteman convention, 861–862

Sanction, 426–427
Sarbanes-Oxley Act 2002, 86
Seamour, Sue, 1037–1040
SEARS Canada Inc., 76–77
Securities and Exchange Commission (SEC), 46
Sellafield nuclear power plant, 44
Selling concept, 484
Senior independent director, 82
Service based audit, 673
Service level agreements, 490
Shareholders, 57–58
constructive use of the AGM, 58
institutional shareholders, dialogue with, 57
Singapore International Money Exchange (SIMEX), 41
Single audit evaluation, 732
Six Sigma program, 713
Smaller listed companies, 85
Smith Report, 135–136
Social audit, 647–650
advertizing standards, 650
business ethics, 649–650
corporate code of conduct, 649–650
denial, 648
environmental auditing, 648
equal opportunities, 650
external image, 647–648
green movement, 649
health and safety, 649
implication, 648–649
pollution, 650
press relationships, 650
Social Ethical and Environmental (SEE), 36
Soft controls, 284–285
Soft systems analysis, 522
Southall Rail Crash, 210
Specifying the job, 718
Speed money, 36
Staff appraisal, 722, 726–728
annual/quarterly plans, 727
audit review process, 726
good appraisal schemes, 728–729
methods of, 726–728
periodic review, 727
reports, 925
Staff discipline, 466
Staff's preferred system, 865–866
Stakeholders, 27–29
responsibilities of, 28
types of, 29
Standardization, 903–904
standardized forms, audit manual, 747–748
Statement of internal control (SIC), 187
Statistical sampling, 909–920
advantages, 911–912
applying to audit process, 913
automated sampling, 915
cluster sampling, 915
compliance test sampling, 916, 918

Statistical sampling (*continued*)
external audit perspective, 909–911
haphazard sampling, 912
interval sampling, 915
judgement sampling, 912
normal distribution, 912
not using, reasons, 910–911
random sampling, 914
rules for applying, 918–920
setting risk parameters, 915–916
stratified sampling, 914
substantive testing sampling, 916–918
Stewardship concept, 25
Stop-go sampling, 918
Strategy versus resources, 792–793
Stratified sampling, 914
Substantive tests, 916
Sumitomo Corporation, 42
Surveillance, 565–566
SWOT analysis, 704–705
opportunities, 705
strengths, 705
weaknesses, 705
threats, 705
System of internal control, 143
Systems auditing, 505–506, 511
Systems-based auditing (SBA), 505
benefits, 516–518
Systems development cycle (SDLC), 603

Technical controls, 801
Temptation, 30–31
Terms of reference, 375
Test data, 630
alternative application, 631
Testing strategies, 877–895
achieving control objectives, 886–888
analytical review, 882–883
compliance and substantive tests, comparing, 880–881
compliance, meaning of, 889–891
100% interrogation theory, 888–889
testing, issues in, 891–892
testing considerations, 881–882
testing process, 877–879
testing techniques, 883–886
types of tests, 879–880
Theft, 548
Three-component model, 346–347
examining independence, 347
programming independence, 346
reporting independence, 347
Three-part model, 362–363
Three-part SD model, 604
Time monitoring systems, 769–771
data owner, 770
input officer, 770
systems controller, 770
systems manager, 770
Tipp-Ex, 550
Traditional audit planning, 808
Traditional tick and check, 369
Transactions approach, 512–513
Transactions testing, 867
Transparency International (TI), 35
Transport for London (TfL), 113
corporate governance assurance, statement of, 113–115
Treadway Commission, 255
Treadway Committee, 127
Trend analysis, 1037
Turnbull Committee, 53
Turnbull Report, risk management, 179–180

UK experience, 49–64
Cadbury, 49–50
combined code, 53
Greenbury, 51–52
Hampel, 52–53
Nolan, 51
Rutteman, 50–51
Turnbull committee, 53
Undercontrol, 253

Value for money (VFM), 100, 322, 642–647, 937
accountability, 644
economy, 642
effectiveness, 642–643
efficiency, 642–643
operations profile, 644
programme, 643–644
Variable sampling, 917
Vinten, Gerald, 1033–1035
Visual aids, 953
Visual aids in formal presentation, 956–957
Vulnerability, 787

Warm standby centres, 620
Whistle-blowing, 37–38, 361–362
Witness, 574–575
Workable system, 866
Working papers, 897–900
audit working paper, 905
be complete, 899
be consistent, 900
be cross-referenced, 898
be economically used, 898
be headed up, 898
be indexed, 898
be signed by the auditor and the reviewer, 899
clearly show any impact on the audit report, 898–899
include summaries wherever possible, 900
indicate which matters are outstanding, 899
objectives of work, 897
professionalism and, 904–905
show any impact on the next audit, 899
show clarity, 898
show the source of information/data, 899
show the work carried out, 899
support the audit decisions/opinion, 898
use pro formas, 898
WorldCom, 45–46

Xerox, 46