

Committee of Sponsoring Organizations of the Treadway Commission

Final draft

Enterprise Risk Management

Integrating with Strategy and Performance

Appendices



June 2017

Volume II

This project was commissioned by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which is dedicated to providing thought leadership through the development of comprehensive frameworks and guidance on internal control, enterprise risk management, and fraud deterrence designed to improve organizational performance and oversight and to reduce the extent of fraud in organizations. COSO is a private sector initiative, jointly sponsored and funded by:

- American Accounting Association
- American Institute of Certified Public Accountants
- Financial Executives International
- Institute of Management Accountants
- The Institute of Internal Auditors

©2017 All Rights Reserved. No part of this publication may be reproduced, redistributed, transmitted, or displayed in any form or by any means without written permission of COSO.

Committee of Sponsoring Organizations of the Treadway Commission

Board Members

Robert B. Hirth Jr.
COSO Chair

Richard F. Chambers
The Institute of Internal Auditors

Mitchell A. Danaher
Financial Executives International

Charles E. Landes
American Institute of Certified Public Accountants

Douglas F. Prawitt
American Accounting Association

Sandra Richtermeyer
Institute of Management Accountants

PwC—Author

Principal Contributors

Miles E.A. Everson
Engagement Leader and Global and Asia, Pacific, and Americas (APA) Advisory Leader
New York, USA

Dennis L. Chesley
Project Lead Partner and Global and APA Risk and Regulatory Leader
Washington DC, USA

Frank J. Martens
Project Lead Director and Global Risk Framework and Methodology Leader
British Columbia, Canada

Matthew Bagin
Director
Washington DC, USA

Hélène Katz
Director
New York, USA

Katie T. Sylvis
Director
Washington DC, USA

Sallie Jo Perraglia
Manager
New York, USA

Kathleen Crader Zelnik
Manager
Washington DC, USA

Maria Grimshaw
Senior Associate
New York, USA

Final Draft

Acknowledgments

The COSO Board and PwC gratefully acknowledge the many individuals who gave their time and energy by participating in and contributing to various aspects of the project. The COSO Board and PwC also recognizes the considerable efforts of the COSO organizations and their members who responded to surveys, participated in workshops and meetings, and provided comments and feedback throughout the development of this framework.

Advisory Council

Douglas J. Anderson
The Institute of Internal Auditors
Managing Director of CAE Solutions

Mark Beasley
North Carolina State University
Deloitte Professor of Enterprise Risk Management and Director, ERM Initiative

Margaret Boissoneau
United Technologies Corporation
PMO Liaison

Anthony J. Carmello
Ernst & Young
Partner, Advisory Services

Suzanne Christensen
Invesco Ltd.
Head of Enterprise Risk

James Davenport
Zurich Insurance Company Global
Head of Risk and Control

James DeLoach
Protiviti Inc.
Managing Director

Karen Hardy
US Department of Commerce
Deputy Director for Risk Management

David J. Heller
Edison International
VP Enterprise Risk Management & General Auditor

Bailey Jordan
Grant Thornton LLP
Partner, Advisory Services

Jane Karli
Athene USA
Director of Investment Operations

James Lam
James Lam & Associates
President

David Landsittel
Former COSO Chair

Lee Marks
First Data Corporation
Enterprise Risk Management

Deon Minnaar
KPMG LLP Americas
Americas Lead Partner for ERM/ GRC

Jeff Pratt
Microsoft
General Manager, ERM

Henry Ristuccia
Deloitte & Touche LLP
Partner, Global Leader - GRC

Paul Sobel
Georgia-Pacific LLC
Vice President/Chief Audit Executive

Patrick Stroh
Mercury Business Advisors Inc.
President

Paul Walker
St. John's University, Tobin College of Business
James J. Schiro / Zurich Chair in Enterprise Risk Management

William Watts
Crowe Horwath LLP
Partner in Charge, Business Risk Services

Final Draft

Observers

Jennifer Bayuk
Citi
Managing Director
Representing International Systems Audit & Controls Association, ISACA

James Dalkin
Government Accountability Office
Director in the Financial Management and Assurance Team

Carol Fox
RIMS, the Risk Management Society
Director, Strategic and Enterprise Risk

Harrison Greene
Federal Deposit Insurance Corporation
Assistant Chief Accountant

Horst Kreisel
Institut der Wirtschaftsprüfer
Director of Project Management

Jeff Thompson
Institute of Management Accountants
President and CEO

Vincent Tophoff
International Federation of Accountants
Senior Technical Manager

Additional PwC Partners and Staff

Julie Bogas
Partner
USA

Lillian Borsa
Partner
USA

Angela Calapa
Director
USA

Juan Carlos Simon
Partner
Mexico

Rick Crethar
Partner
Australia

Symon Dawson
Partner
UK

David Fisher
Partner
USA

Tobias Flath
Senior Manager
Germany

Peter Frank
Partner
USA

Dimitriy Goloborodskiy
Partner
USA

Rob Gormly
Partner
USA

Carmen Le Grange
Partner
South Africa

Christof Menzies
Partner
Germany

Gonzalo Nunez
Partner
Mexico

Jason Pett
Partner
USA

Marcel Prinsenberg
Senior Manager
Netherlands

Jerri Ribeiro
Partner
Brazil

Jonathan Riva
Partner
Canada

Nicole Salimbeni
Partner
Australia

David Sapin
Partner
USA

Manuel Seiferth
Senior Manager
Germany

Dietmar Serbee
Partner
USA

Laurie Schive
Director
USA

Stephen Soske
Partner
USA

Christina Stecker
Partner
Germany

Olivier Sueur
Senior Manager
Netherlands

Kuntal Sur
Partner
India

Alywin Teh
Partner
Singapore

Armando Urunuela
Partner
Mexico

Steven van Agt
Senior Manager
Netherlands

Kosta Weber
Partner
Netherlands

Andrew Wilson
Partner
Australia

Stephen Zawoyski
Partner
USA

Additional Contributors

PwC also wishes to thank Geoffrey Albutt, Catherine Jordan, Mark Tan, and Karen Vitale for their contributions to the development of the Framework.

Final Draft

Table of Contents

A. Project Background and Approach for Revising the Framework 1

B. Summary of Public Comments 3

C. Roles and Responsibilities for Enterprise Risk Management 9

D. Risk Profile Illustrations 17

Final Draft

Final Draft

A. Project Background and Approach for Revising the Framework

Project Background

In October 2014, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) announced that it would be reviewing and updating the 2004 *Enterprise Risk Management–Integrated Framework* (original Framework). The original Framework is widely accepted and used by management and boards to enhance an organization's ability to manage uncertainty and to consider how much risk to accept as they strive to increase stakeholder value.

Since 2004, the complexity of risk has changed, significant new risks have emerged, and boards have enhanced their awareness and oversight of risk management while asking for improved risk reporting. Updates to the Framework reflect current and evolving concepts and applications so that organizations worldwide can attain better value from enterprise risk management. Specifically, it now provides greater insight into strategy and the role of enterprise risk management in the setting and execution of strategy, enhances the alignment between organizational performance and enterprise risk management, and accommodates expectations for governance and oversight.

PwC served as the author and project leader for updating the publication, preparing related documents and reporting to the COSO Board of Directors. The PwC Project Team includes senior resource people, many who were involved in previous COSO projects and who bring in-depth understanding of the original Framework, and others who provide current market perspectives to this revision. To capture views of a broad range of professionals in the marketplace, the COSO Board formed an Advisory Council representing industry, academia, government agencies, and not-for-profit organizations and invited Observers to attend Advisory Council meetings.

Approach for Revising the Framework

The PwC Project Team carefully considered the merits of feedback and opinions received throughout the project. They reviewed and embraced input that helped in the development of a relevant, logical, and internally consistent document in all phases of the project. These phases include:

- *Assess and Envision:* Through literature reviews, global surveys, and public round tables and forums, this phase identified current challenges for organizations implementing enterprise risk management. The PwC Project Team analyzed information, reviewed various sources of input, and identified critical issues and concerns. COSO launched a global survey, available to the general public, for providing input on the original Framework, soliciting almost 900 responses.

Final Draft

- *Build and Design:* The PwC Project Team drafted *Enterprise Risk Management–Aligning Risk with Strategy and Performance*,[1] which was reviewed by the COSO Advisory Council and Observers as well as other key users to gather reactions and suggestions. The PwC Project Team conducted numerous one-on-one and group meetings to capture feedback on the alternative directions being considered in drafting the Framework. These meetings, conducted across North America, Europe, Asia, and Australia, included board members, chief risk officers, chief financial officers, chief audit executives, and other senior members of management.
- *Public Exposure:* With the assistance and oversight of the COSO Board, PwC prepared exposure drafts and an on-line questionnaire to facilitate a review by the general public. The PwC Project Team conducted a variety of meetings and presented at conferences to capture added input. Appendix B presents a summary of the public comments and the Project Team's response.
- *Finalization:* The PwC Project Team reviewed and analyzed all comments received and refined the various documents with needed modifications. The COSO Board considered whether *Enterprise Risk Management–Integrating with Strategy and Performance* was sound, logical, and useful to management of entities of all types and sizes, and the PwC Project Team finalized the document for the COSO Board for acceptance.

Final Draft

1 This working title was used throughout the public exposure phase, and then the document was retitled *Enterprise Risk Management–Integrating with Strategy and Performance*.

B. Summary of Public Comments

As noted in Appendix A, a draft of the Framework was issued for public comment from June 15 through September 30, 2016. There was significant interest in the exposure draft, indicated by almost 10,000 downloads[2] of the Framework across industries and from entities of all types. Much of the interest was international: 46% of downloads occurred from outside North America.

There were forty-eight public comment letters received and more than 200 responses to the on-line survey to the exposure draft. The public comment letters generated more than 1,600 comments and the on-line survey resulted in over 400 free-form responses on many aspects of the updated document. All comments were considered in further revisions to the Framework.

In addition to the feedback generated from COSO, the PwC Project Team solicited feedback from the public through over forty meetings, conferences, and seminars during the public exposure period. In addition, they developed a series of videos, articles on key topics (e.g., managing risk and performance to support strategy), and social media posts, which generated over 2.8 million impressions and over 3,000 direct interactions from the public.

This appendix summarizes the more significant comments and resulting modifications to the Framework arising from the public exposure period. Many respondents supported COSO's efforts to update the Framework to emphasize the importance of considering risk in both strategic planning and overall performance, add five components of enterprise risk management, and stress how integrating enterprise risk management into the business can improve decision-making.

However, there were divergent views on certain updates to the Framework, including the definitions of risk and enterprise risk management, the link to decision-making, the practicality of risk profiles, and the relationship of internal control to enterprise risk management.

Some respondents sought fundamental changes to the Framework, whereas others recognized that the Framework remains relevant and useful today for boards and management of entities regardless of type or size, and requested that only specific areas be updated, as discussed in more detail below.

Structuring the Document: Components and Principles

Overall, respondents supported updating the original title of the Framework, *Enterprise Risk Management–Aligning Risk with Strategy and Performance*. They acknowledged the benefits of a components and principles structure to provide clarity to integrating enterprise risk management into strategic planning and day-to-day decision-making. Some suggested the five components of the Framework could be better aligned with a common business model of develop, implement, review, and revise. Further, some noted that the use of the word "execution" in the Risk in Execution component did not translate well across geographies. A few respondents expressed concern about the number of principles, saying twenty-three was not practical for managing an entity, and suggested having fewer. Lastly, others suggested changes to align or reconcile the Framework principles to other frameworks and standards.

Given the overall support of integrating enterprise risk management with strategy-setting through performance, the title was revised to *Enterprise Risk Management–Integrating with Strategy and Performance*. The Framework retains the five components but renames and reorders them to better align to a typical business model: Governance and Culture; Strategy and Objective-Setting; Performance; Review and Revision; and Information, Communication, and Reporting.

2 Downloads from the COSO.org website

Final Draft

As for the principles, some have been consolidated. Specifically, two principles within the Governance and Culture component were combined into one to focus on core values. As well, within the Strategy and Objective component, the principles Considers Risk while Establishing Business Objectives and Defines Acceptable Variation in Performance were merged into one, Formulates Business Objectives, which focuses on establishing objectives and using tolerance to understand how risk impacts the achievement of those objectives. Lastly, within the Information, Communication, and Reporting component, the principles Use Relevant Information and Leverages Information Systems were merged into one to focus on information and technology supporting enterprise risk management practices.

Some respondents also expressed concern about the length of the document and complexity of the language. Specifically, they requested greater use of plain language to make certain technical terms accessible to a wider audience.

These concerns were addressed by consolidating principles as discussed above. Additionally, the Framework was revised to reduce sentence length to improve readability. Specifically, the Flesch–Kincaid readability tool was used to identify areas for improvement as well as to confirm the readability for similar standards and frameworks. Given the complexity of certain topics, the overall Framework remains a comprehensive document in length to sufficiently develop and clarify concepts.

Final Draft

Defining Enterprise Risk Management and Risk

Respondents provided various suggestions to amend the definitions of risk and enterprise risk management, including aligning the definitions with other frameworks and standards. Suggestions for defining risk varied from including impact only, separating risk into adverse events (threats) and opportunities, and focusing on uncertainty.

Some respondents expressed preference for the 2004 definition of enterprise risk management, in particular the use of risk appetite, roles and responsibilities, and a focus on processes, as opposed to practices. Others preferred the exposure draft definition and requested incorporating decision-making into it. There were also requests to condense the definition by removing "creating, preserving, realizing value" and providing a clear separation between risk management and enterprise risk management.

After careful review and analysis of definitions from other standards and frameworks, it was decided the exposure draft's definitions would be kept. The COSO Board believes those definitions best reflect COSO's present view of risk and enterprise risk management and align with other COSO frameworks and thought leadership.

Integrating Enterprise Risk Management and Impact on Decision-Making

A number of respondents expressed support for integrating enterprise risk management with core business activities, as opposed to having a more process-based approach. Some viewed enterprise risk management as more of a function (e.g., second line of defense), as opposed to a capability. As part of integrating enterprise risk management, respondents requested an expanded discussion on decision-making throughout the Framework, including the role of bias and risk appetite, and a stronger connection to culture.

Given the focus on capabilities and practices as opposed to a specific function, the Framework contains limited discussion on the lines-of-defense model. Further discussion on roles and responsibilities is included in Appendix C.

The Framework now includes a new chapter, "Integrating Enterprise Risk Management", which focuses on how enterprise risk management is integrated with strategy-setting through performance, and the value of integration for the entity, such as improved decision-making. The new chapter and each principle in the Framework enhance the discussion of decision-making and the impact of management bias.

The Relationship of Enterprise Risk Management to Internal Control

There was diverse feedback on the relationship between enterprise risk management and internal control. Some respondents requested clarification of the structural aspects of the two frameworks (e.g., where there is overlap) and the conceptual linkages of these two topics. Some suggested COSO merge the two frameworks into one, while others preferred two separate and distinct frameworks. Still others suggested including the entirety of the internal control conversation in the Framework rather than referencing *Internal Control–Integrated Framework*.

The new Framework now clarifies the relationship between enterprise risk management and internal control and identifies those instances where it relies on concepts established in *Internal Control–Integrated Framework*. Since *Internal Control–Integrated Framework* is used as a regulatory standard, and to avoid inadvertently expanding the scope of that framework for regulatory application, the COSO Board decided to maintain two separate and distinct frameworks. Therefore, the COSO Board did not include components in this update that are common to both frameworks (e.g., control activities) to avoid redundancy and to encourage users to become familiar with both. However, some concepts introduced in *Internal Control–Integrated Framework*, such as governance of enterprise risk management, are further developed in this Framework. These additions limited the ability to shorten the document.

Discussion on Strategy

Respondents expressed overall support for the emphasis on strategy throughout the Framework. Some requested clarity on the transition from strategy planning to implementation and when to revisit strategy. A few held the view that objectives precede strategy, and others requested replacing strategy with strategic objectives. There were varying opinions about including the setting of mission, vision, and core values within the scope of enterprise risk management.

The Framework retains the current focus on the "possibility of strategy not aligning, implications from the strategy chosen, and risks to performing the strategy" as these provide a more detailed analysis of the importance of integrating enterprise risk management with strategy-setting. The Framework now clarifies how enterprise risk management is applied across strategy and performance. It retains the link to mission, vision, and core values as that provides the foundation of the acceptable type and amount of risk. Additionally, the Framework retains the hierarchy relationship between strategy and business objectives, and the terminology of strategy versus strategic objectives, as both are consistent with commonly used strategy and business frameworks.

Final Draft

Role of Culture

Overall, there was positive support for the inclusion and prominence of culture in the exposure draft. Some respondents suggested further expanding the discussion on the culture spectrum and emphasizing links to performance management, conduct, and incentives. A few suggested that culture is not part of the definition of enterprise risk management, while others suggested that entities do have a culture and risk is a part of it. Some wanted a discussion on fraud risk as it relates to culture.

The Framework has been revised to consolidate Principles 4, 5, and 6 into the new Principle 4, Demonstrates Commitment to Core Values. This principle emphasizes the relationship between enterprise risk management and the core values established by the board and management for the entity. Additionally, the revised Framework is enhanced with examples of how culture influences enterprise risk management practices and decision-making, including the influence of management bias. It does not include discussions of fraud risk, as this is addressed in *Internal Control–Integrated Framework*.

Risk Appetite and Tolerance

Several respondents took a risk-centric view to risk appetite, as opposed to an objective-centric view. Related comments focused on setting boundaries for specific risks or groups of common risks (e.g., credit risk) and reinforced a view of managing risk through discrete groups. Further, several respondents requested that the discussion on risk appetite be revised to make it measurable for specific risks instead of focused on decision-making. Others requested a visual diagram, demonstrating the hierarchy of risk appetite and tolerance.

The Framework retains the use of risk appetite in the development of strategy and business objectives, and the emphasis on how it is used in decision-making. A diagram has been added to clarify the relationship between risk appetite, tolerance, and limits and triggers, and how those elements apply to strategy, objectives, and specific risks.

Respondents also questioned the use of acceptable variation in performance in lieu of risk tolerance. In particular, some strongly expressed a desire to revert to using risk tolerance from the 2004 Framework, while others noted the use of acceptable variation in performance as an improvement. The final Framework has revised the use of acceptable variation in performance to tolerance and enhanced the discussion on how tolerance is tied to an entity's objectives, taking an objective-centric view.

Risk Assessment and Risk Profiles

Some feedback targeted the technical risk assessment practices, including the use of risk profiles. Specifically, several respondents requested a more detailed discussion of quantitative risk assessment methods (e.g., modeling, simulations, decision trees) and other practical tools. Some expressed concern about the value of heat maps, arguing that they are typically risk-centric and do not accurately reflect the relationship of risk with performance. Several noted the absence of discussion on the distribution of outcomes, while many questioned the inclusion of inherent risk assessments.

Final Draft

The final Framework has revised Principle 11, Assess Severity of Risk, to focus more explicitly on the impact to the achievement of business objectives and strategy. It also clarifies how heat maps can be used to depict risk in the context of objectives. Additionally, a discussion on quantitative approaches to risk assessments was added.

Some respondents questioned the practical application of risk profiles, whereas others noted limiting the risk profile to one graphic may be too prescriptive. Those supportive of the risk profiles noted that they provide an effective explanation of the relationship between risk, performance targets, risk capacity, and risk appetite.

The final Framework retains the use of risk profiles as they provide management with a view of how risk impacts performance and how risk appetite can be used for decisions. Enhancements have been made to clarify the risk profile graphics across different types of business objectives, and how risk profiles can be used with both qualitative and quantitative data.

Information and Technology

Some respondents requested a detailed discussion on information and technology; others questioned whether data management and technology were within the scope of enterprise risk management. Several focused on reporting information from a risk-centric perspective as opposed to business viewpoint.

The Framework now has a revised Information, Communication, and Reporting component to reduce the focus on information systems and put more emphasis on the greater role of data and evolving technology as part of enterprise risk management. Specifically, information has been added on how an entity manages and analyzes data, and the use of evolving technology to manage data more efficiently and effectively. The Framework also now highlights objective-based reporting to support management in decision-making.

Guidance

Some respondents requested guidance on how a company could apply the concepts discussed in the Framework. Specifically, they asked for more examples, including mini or full case studies, tools to assist in evaluating enterprise risk management (e.g., maturity models), and general implementation guidance (e.g., risk reports).

In response, the COSO Board and the PwC Project Team agreed to develop a separate document containing examples on applying the Framework, *Enterprise Risk Management–Integrating with Strategy and Performance*: *Compendium of Examples*. This document illustrates the application of all the principles in the Framework across different industries, entity sizes, and types, and actual and expected company practices.

Final Draft

Final Draft

C. Roles and Responsibilities for Enterprise Risk Management

In any entity, everyone shares responsibility for enterprise risk management. The leader of the entity (i.e., chief executive officer or president) is ultimately responsible and should assume ownership for the achievement of the entity's strategy and business objectives. That person should also have a deep understanding of those factors that may impede the achievement of strategy. It is up to other managers to "live and breathe" the behaviors that align with the culture, oversee enterprise risk management, leverage information systems tools, and monitor performance. Other personnel are responsible for understanding and aligning to the cultural norms and behaviors, business objectives in their area, and related enterprise risk management practices. The board of directors provides risk oversight to the achievement of strategy.

This appendix looks at approaches an organization can take for assigning roles and responsibilities for enterprise risk management, and provides guidance on the roles and responsibilities of the board of directors, chief executive officer, chief risk officer, management, and internal auditor. The information is presented in a "lines of accountability model."

The lines of accountability model offers an organization a balanced approach to managing risk and seizing opportunities, all while enabling risk-based decision-making that is free of bias. However, there is no one-size-fits-all approach to using this model and no prescriptive details on the number of lines of accountability necessary. Some industries offer specific guidance for implementing an accountability model, but organizations must consider factors such as their size, strategy and business objectives, organizational culture, and external stakeholders. Individual organizations may establish roles across any number of different lines of accountability with specific regulatory guidance and oversight. Regardless of the number of lines of accountability, the roles, responsibilities, and accountabilities are defined to allow for clear "ownership" of strategy and risk that fits within the governance structure, and culture of the entity.

Board of Directors and Dedicated Committees

Different entities will establish different governance structures, such as a board of directors, a supervisory board, trustees and/or general partners, and dedicated committees. In the Framework (Chapters 5 through 9), these governance structures are commonly referred to generally as "the board of directors."

The board of directors is responsible for providing risk oversight of enterprise risk management culture, capabilities, and practices. Therefore, board members must be objective, capable, and inquisitive. They should have technical knowledge and expertise that is relevant to the entity's operations and environment, and they must commit to the time necessary to fulfill their day-to-day risk oversight responsibilities and accountabilities. In some jurisdictions, the board has legal responsibility for carrying out its oversight role. Figure C.1 lists typical board oversight practices of enterprise risk management.

Final Draft

Figure C.1: Board Oversight Activities

Enterprise Risk Management Component	Board Risk Oversight Activities
Governance and Culture	• Assesses the appropriateness of the entity's strategy, alignment to the mission, vision, and core values, and the risk inherent in that strategy. • Defines the board risk governance role and structure including sub-committees for the entity. • Engages with management to define the suitability of enterprise risk management. • Oversees evaluations of the entity's culture and that management remediates any noted gaps. • Promotes a risk-aware mindset that aligns the maturity of the entity with its culture. • Oversees the alignment of business performance, risk taking, and incentives/compensation to balance short-term and long-term strategy achievement. • Challenges the potential biases and organizational tendencies of management and fulfills its independent and unbiased oversight role. • Understands the entity's strategy, operating model, industry, and issues and challenges affecting the entity. • Understands how risk is monitored by management.
Strategy and Objective-Setting	• Sets expectations for integrating enterprise risk management into the strategic management processes, including strategy planning, capital allocation, etc. • Discusses and understands the risk appetite and considers whether it aligns with its expectations. • Engages in discussion with management to understand the changes to business context that may impact the strategy and its linkage to new, emerging, or manifesting risks. • Encourages management to think about the risks inherent in the strategy and underlying business assumptions. • Requires management to demonstrate an understanding of the risk capacity of the entity to withstand large, unexpected events.

Final Draft

Figure C.1—Continued

Enterprise Risk Management Component	Board Risk Oversight Activities
Performance	• Reviews the entity's strategy and underlying assumptions against the portfolio view of risk. • Sets expectations for risk reporting, including the risk metrics reported to the board relative to the risk appetite of the entity and external enterprise risk reporting disclosures. • Understands how management identifies and communicates the most severe risks as depicted by the entity's portfolio view. • Reviews and understands the most significant risks, including emerging risks, and significant changes in the portfolio view of risk and specifically what responses and actions management is taking. • Understands the plausible scenarios that could change the portfolio view.
Review and Revision	• Asks management about any risk manifesting in actual performance (both positive and negative). • Asks management about the enterprise risk management processes and challenges management to demonstrate the suitability and functioning of those processes.
Information, Communication, and Reporting	• Identifies information, underlying data, and formats (graphs, charts, risk curves, and other visuals) required to execute board oversight. • Accesses internal and external information and insights conducive to effective risk oversight. • Obtains input from internal audit, external auditors, and other independent parties regarding management perceptions and assumptions.

The board of directors may choose to manage its risk oversight responsibilities at the full board level or may assign specific tasks to dedicated committees with a risk focus. Where a particular committee has not been established for risk oversight, the responsibilities are carried out by the board itself.

Board-level committees can include the following:

- *Audit committee:* Establishes the importance of risk oversight. Regulatory and professional standard-setting bodies often require the use of an audit committee, sometimes named the audit and risk committee. The role and scope of authority of an audit committee can vary depending on the entity's regulatory jurisdiction, industry norm, or other variables. While management is responsible for ensuring financial statements are reliable, an effective audit committee plays a critical risk oversight role. The board of directors, often through its audit committee, has the authority and responsibility to question senior management on how it is carrying out its enterprise risk management responsibilities.
- *Risk committee:* Establishes the direct oversight of enterprise risk management. The focus of the risk committee is entity-wide risk in non-financial areas that go beyond the authority of the audit committee and its available resources (e.g., operational, obligations, credit, market, technology).
- *Compensation committee:* Establishes and oversees the compensation arrangements for the chief executive officer and other executives, as appropriate, to motivate without providing incentives for undue risk taking. It also oversees that management balances

Final Draft

performance measures, incentives, and rewards with the pressures created by the entity's strategy and business objectives, and helps structure compensation models without unduly emphasizing short-term results over long-term performance.

- *Nomination/governance committee:* Provides input to and oversight of the selection of candidates for directors and management. It regularly assesses and nominates members of the board of directors; makes recommendations regarding the board's composition, operations, and performance; oversees the succession-planning process for the chief executive officer and other key executives; and develops oversight processes and structures. It also promotes director orientation and training, and evaluates oversight processes and structures (e.g., board/committee evaluations).

Management and the Three Lines of Accountability

Management is responsible for all aspects of an entity, including enterprise risk management. Responsibilities assigned to the various levels of management are outlined here.

Chief Executive Officer

The chief executive officer (CEO) is accountable to the board of directors and is responsible for overall enterprise risk management culture, capabilities, and practices required to achieve the entity's strategy and business objectives. (In privately owned and not-for-profit entities, this position may have a different title, but generally the responsibilities are the same.) More than any other individual, the CEO sets the tone at the top along with the explicit and implicit values, behaviors, and norms that define the culture of the entity.

The CEO's responsibilities relating to enterprise risk management include:

- Providing leadership and direction to senior members of management, and shaping the entity's core values, standards, expectations of competence, organizational structure, and accountability.
- Evaluating alternative strategies, choosing a strategy, and setting business objectives that consider supporting assumptions relating to business context, resources, and capabilities within the risk appetite of the entity.
- Maintaining oversight of the risks facing the entity (e.g., directing all management and other personnel to proactively identify, assess, prioritize, respond to, and report risks that may impede the ability to achieve the strategy and business objectives).
- Guiding the development and performance of the enterprise risk management process across the entity, and delegating to various levels of management at different levels of the entity.
- Communicating expectations (e.g., integrity, competence, key policies) and information requirements (e.g., the type of planning and reporting systems the entity will use).

Chief Risk Officer

One of the more prominent roles in enterprise risk management is that of chief risk officer (CRO). This position is tasked with overseeing enterprise risk management as a second line of accountability. This role should normally have reasonably direct access to the CEO, or the authority to have access for specific issues or types of risk. An alternative to having a chief risk officer is to assign the underlying responsibilities to another member of management, typically in the second line of accountability.

Final Draft

Organizations develop the CRO role and responsibilities in a way that best meets their needs for effective enterprise risk management. Some entities choose to align the role of chief risk officer with the chief strategy officer so that strategy and risk are managed together under the CEO. Other entities delegate responsibility for enterprise risk management to first-line functions, including operating unit and functional unit leaders, leaving second-line responsibility to the CRO. These entities often align staff within divisions, operating units, and functions with the CRO to support enterprise risk management efforts across the entity.

The CRO is typically responsible for:

- Assisting the board of directors and management in fulfilling their respective risk oversight responsibilities.
- Establishing ongoing enterprise risk management practices suitable for the entity's needs.
- Building and maintaining relationships with those responsible for managing risks throughout the entity.
- Overseeing enterprise risk management ownership within the respective lines of accountability.
- Reviewing the operation of enterprise risk management in each operating unit.
- Communicating with management through a forum, such as the enterprise risk management committee, about the status of enterprise risk management, which includes discussing severe risks and emerging risks.
- Promoting enterprise risk management to the CEO and operating unit leaders and assisting in integrating practices into their business plans and reporting.
- Evolving organizational capabilities in line with the maturity and suitability of enterprise risk management.
- Escalating identified or emerging risk exposures to executive management and the board.

Management

Management comprises the CEO and senior members leading the key operating units and business-enabling functions. Each of these management roles may have different responsibilities and accountabilities within the lines of accountability model, depending on the entity. For example, a chief technology officer may play a second-line role in a financial services company, but in a technology company that same position would play a first-line role. Some smaller entities may combine roles, with one person having responsibilities for one or more. Examples of management for a larger public or private entity, a smaller business entity, and a government entity are noted in Figure C.2.

Final Draft

Figure C.2: Management Roles within Different Entities

Large Public/Private Entity	Small Business Entity	Governmental Entity
• Chief executive officer and president • Chief administrative officer • Chief audit executive • Chief compliance officer • Chief data officer • Chief financial officer • Chief human resources officer • Chief information officer • Chief innovation officer • Chief legal officer/general counsel • Chief marketing officer • Chief operating officer • Chief risk officer • Chief strategy officer	• President • Chief financial officer/vice president (VP) of finance/ finance director/head of finance/controller • Chief operating officer • Director of risk management/ head of risk management • General manager/VP of operations • Human resources manager/ director • IT manager • Marketing manager	• Secretary • Assistant secretary/deputy director/undersecretary • Chief financial officer • Chief information officer • Chief of human resources • Chief of staff • Deputy assistant secretary/ directorate • Director of risk management/ head of risk management • General counsel • Inspector general

In some entities, the CEO establishes an enterprise risk management committee of senior members of management including functional managers, such as the chief financial officer, chief audit executive, chief information officer, and others. Examples of the functions and responsibilities of such a committee include:

- Assuming overall responsibility for enterprise risk management, including the processes used to identify, assess, prioritize, respond to, and report on risk.
- Communicating the enterprise risk management process to the CEO and the board.
- Considering and discussing emerging risks.
- Defining roles, responsibilities, and accountabilities at the different levels of management.
- Providing policies, methodologies, and tools to operating units to identify, assess, and manage risks.
- Reviewing the entity's risk profile.
- Reviewing acceptable variation in performance and taking action where appropriate.

Management also guides the development and implementation of enterprise risk management practices within their respective functional or operating unit and verifies that these practices are applied consistently.

Depending on how many layers of management exist within an entity, subunit managers or lower-level supervisory personnel are directly involved in executing policies and procedures at a detailed level. It is their responsibility to carry out the enterprise risk management process that

Final Draft

senior management has designed and implemented. Each manager is accountable to the next higher level for his or her portion of enterprise risk management, with the CEO being ultimately accountable to the board of directors, and the board being accountable to external stakeholders such as shareholders or other owners of the entity.

First Line: Core Business

Management is responsible for identifying and managing the performance and risks resulting from practices and systems for which it is accountable. The first line is also responsible for the risks inherent to the strategy and business objectives. As the principal owners of risk, management sets business objectives, establishes acceptable variation in performance, trains personnel, and reinforces risk responses. In short, the first line implements and carries out the day-to-day tasks to manage performance and risks taken to achieve strategy and business objectives.

Second Line: Support Functions

Support functions (also referred to as business-enabling functions) include management and personnel responsible for overseeing performance and enterprise risk management. They provide guidance on performance and enterprise risk management requirements, and evaluate adherence to defined standards. Each of these functions has some degree of independence from the first line of accountability, and they challenge the first line to manage performance and take prudent risks to achieve strategy and business objectives. In some entities, independent teams without separate and distinct reporting lines may provide some degree of challenge. These organizational functions or operating units support the entity through specialized skills, such as technical risk management expertise, finance, product/service quality management, technology, compliance, legal, human resources, and others. As management functions they may intervene directly in modifying and supporting the first line in appropriate risk response.

Second-line responsibilities often include:

- Supporting management policies, defining roles and responsibilities, and setting targets for implementation.
- Providing enterprise risk management guidance.
- Supporting management to identify trends and emerging risks.
- Assisting management in developing processes and risk responses to manage risks and issues.
- Providing guidance and training on enterprise risk management processes.
- Monitoring the adequacy and effectiveness of risk responses, accuracy, and completeness of reporting, and timely remediation of deficiencies.
- Escalating identified or emerging risk exposures to management and the board for awareness and potential action.

There are various methods of achieving objectivity across these two lines of accountability. For example, one company may have enterprise risk management teams embedded in the first line but with a separate second-line risk function. Another company may spread its risk management teams across the two lines depending on the complexity and nature of the business. These and other approaches can work as long as unbiased oversight is not constrained.

Final Draft

Third Line: Assurance Functions

Assurance functions, most commonly internal audit, often provide the last line of accountability by performing audits or reviews of enterprise risk management practices, identifying issues and improvement opportunities, making recommendations, and keeping the board and executive management up-to-date on matters requiring resolution. Two factors distinguish the last line of accountability from the others: the high level of independence and objectivity (enabled by direct reporting to the board), and the authority to evaluate and make recommendations to management on the design and operating effectiveness of the entity overall.

External Auditors

External auditors provide management and the board of directors with a unique, independent, and objective view that can contribute to an entity's achievement of its strategy and business objectives.

In an external audit, the auditor expresses an opinion on the fairness of the financial statements in conformity with applicable accounting standards, thereby contributing to the entity's external financial reporting objectives. The auditor conducting a financial statement audit may contribute further to those objectives by providing information useful to management in carrying out its enterprise risk management responsibilities. Such information includes:

- Audit findings, analytical information, and recommendations for actions necessary to achieve established business objectives.
- Findings regarding deficiencies in enterprise risk management and internal control that come to the auditor's attention, and recommendations for improvement.

This information frequently relates not only to reporting but to strategy, operations, and compliance practices as well, and can be important to an entity's achievement of its business objectives. The information is reported to management and, depending on its significance, to the board of directors or audit committee.

It is important to recognize that a financial statement audit, by itself, normally does not include a significant focus on enterprise risk management. Nor does it result in the auditor forming an opinion on the entity's enterprise risk management. Where, however, law or regulation requires the auditor to evaluate a company's assertions related to internal control over financial reporting and the supporting basis for those assertions, the scope of the work directed at those areas will be extensive, and additional information and assurance will be gained.

Final Draft

D. Risk Profile Illustrations

Introduction to Risk Profiles

A risk profile provides the composite view of risks related to a specific strategy or business objective at a particular level of the entity (e.g., overall entity level, business unit level, functional level) or aspect of the business model (e.g., product, service, geography). These risk profiles bring together several important considerations in enterprise risk management, namely performance targets, the assessment of the overall amount of risk for varying levels of performance, risk appetite, and tolerance. Risk profiles are used to help organizations evaluate alternative strategies and support the process of identifying and assessing risks.

This relationship between risk and performance is rarely constant. Changes in performance do not always result in corresponding changes in risk, and therefore a single-point illustration used in many typical enterprise risk management approaches is not always helpful. A more complete illustration shows the aggregate amount of risk associated with different levels of performance, where risk is shown as a continuum of potential outcomes. The organization balances the amount of risk with desired performance along this continuum.

This appendix offers examples of how risk profiles may be developed and applied to support the organization in applying the principles of the Framework.

Developing Risk Profiles

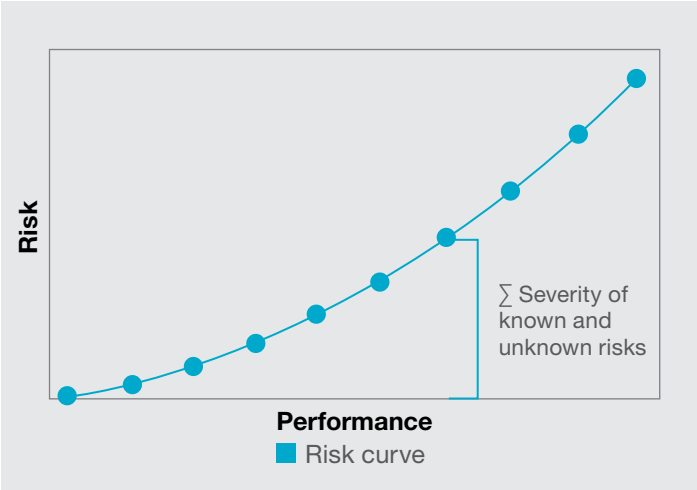
When developing a risk profile, the organization must understand the:

- Strategy or relevant business objective.
- Performance target and acceptable variances in performance.
- Risk capacity and appetite for the entity.
- Severity of the risk to the achievement of the strategy and business objective.

The risk profile, as depicted in this appendix, enables the organization to evaluate:

- The relationship between risk and performance, noting that the amount of risk for a given strategy or business objective is typically not static and will change for different levels of performance.
- Assumptions underlying the risk assessment for a given strategy or business objective.
- The level of confidence with which the assessment has been performed and the potential for unknown risks.
- Where corrective actions may be required in setting strategy, business objectives, performance targets, or risk responses.

Figure D.1: Risk Profile



Final Draft

To develop a risk profile, the organization determines the relationship between the level of performance for a strategy or business objective and the expected amount of risk. On a risk graph, performance is plotted along the x-axis and risk is along the y-axis (Figure D.1). The resulting line is often referred to as a "risk curve" or "risk profile."

Each data point is plotted by considering the perceived amount of risk that corresponds to the achievement of a business objective or strategy. As performance changes, the organization identifies how the amount of risk may change. Risk may change due to the changes in execution and business context.

Both quantitative and qualitative approaches can be used to plot points. If the organization has sufficient data on a strategy or business objective, it may use a quantitative approach, such as probabilistic modeling or regression analysis. Where data is not available or where business objectives are less important, the organization may prefer to use a qualitative approach, such as performing interviews, facilitating workshops, or benchmarking. Example D.1 describes how one entity plotted its risk profile.

Example D.1: Developing a Risk Profile

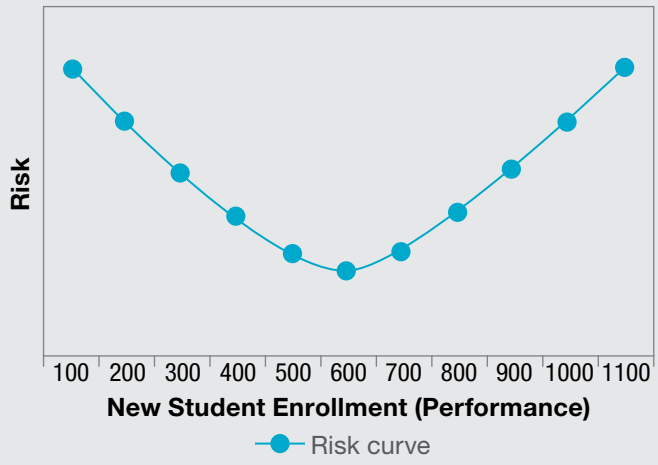
A university has a strategy of becoming the institution of choice for graduate students in the region. To support the strategy, it has decided on a business objective of developing a new curriculum to meet emerging needs. The university has identified the following five risks for this business objective:

- Failing to build sufficient interest and awareness of the courses to generate growth in student applications, which could impact the university's reputation.
- Generating actual or perceived conflict of interest between academic freedom and the new curriculum.
- Failing to attract and retain additional faculty required to teach and administer new classes.
- Failing to secure additional government funding to administer the new curriculum.
- Incurring unbudgeted costs in support of the new curriculum.

In addition, the university has identified that this new objective creates potential risk to other objectives, such as the possibility of marginal students affecting the university's brand.

The university measures performance based on the number of student enrollments. It assesses the severity of the risks to the achievement of the business objective changes at various levels of student enrollment. That is, the distance between the point and the x-axis represents the impact of the five risks identified, as depicted on the right. For each level of student enrollment, the university considers the following:

- How might some risks escalate across varying levels of performance? For instance, the risk of attracting faculty may increase at higher levels of enrollment as more instructors may be required.



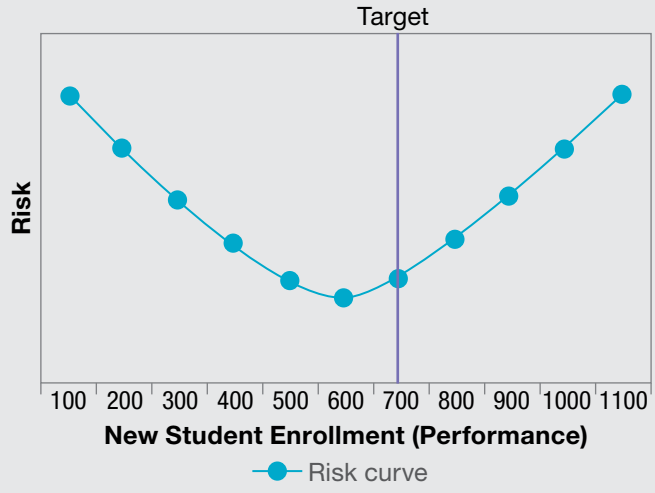
Final Draft

- How might risks change in severity and what supporting assumptions may change at varying levels of performance? For instance, assumptions of government funding may be contingent on achieving set levels of enrollment.
- Are there new or emerging risks with each incremental increase in student enrollment? For instance, does enrollment above a certain level create a new risk relating to the physical space required to accommodate students?
- Are there some risks that no longer apply at certain levels of performance? For instance, do the concerns about failing to generate sufficient interest and awareness of the university's courses become increasingly irrelevant above a certain level of enrollment?

In preparing this profile, the university uses a combination of quantitative and qualitative approaches. Quantitative approaches include data modeling (reviewing historical student enrollments and correlation with the launch of new programs, the average number of operational incidents, revenues and losses per student). Qualitative approaches include reviewing campus health and safety requirements, forecasting revenue and government grants, and conducting interviews and workshops with key stakeholders. The risk profile shown on below illustrates that:

- There is a high amount of risk assumed if only 100 new students enroll because of the new curriculum (risk of underperformance).
- Risk reaches its lowest point at 600 enrollments, which may not represent the optimal number of students from a performance perspective.
- Any enrollments in excess of 600 represent an incremental increase in risk. The university has established that it can accept a maximum of 1,100 new students.

Having determined how the amount of risk can change, and understanding the drivers and assumptions that support change, the organization can determine its desired performance target. To set that target, the organization evaluates the business objective in the context of the entity's risk appetite, resources, and capabilities. In the case described above, the university ultimately decides that it will set a performance target of seeking to attract 700 new students. The risk profile above illustrates this target and the amount of risk the university is willing to assume in the pursuit of the objective.



Final Draft

Risk, Strategy, and Objective-Setting

Incorporating Risk Appetite

Using a risk profile, the organization can outline its risk appetite in relation to a proposed strategy or business objective. In Figure D.2, the risk appetite is plotted as horizontal line parallel to the x-axis (performance). The gradient of the line indicates that the risk appetite remains constant for all levels of performance at a given point in time. The y-axis (risk) uses the same metric or expression of risk appetite as is referred to in an entity's risk appetite statement. For example, the y-axis may be earnings at risk, value at risk, or other metric.

The section of the curve from the point of intersection (Point A) where it continues above the risk appetite line indicates a level of performance that exceeds the entity's appetite and where risk becomes disruptive to the entity.

Organizations may also want to incorporate an additional parallel line above risk appetite to indicate risk capacity, shown in Figure D.3.

Figure D2: Risk Profile with Risk Appetite

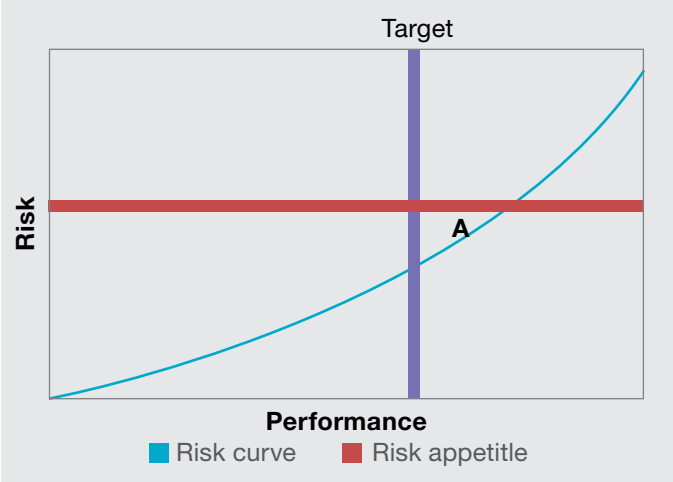
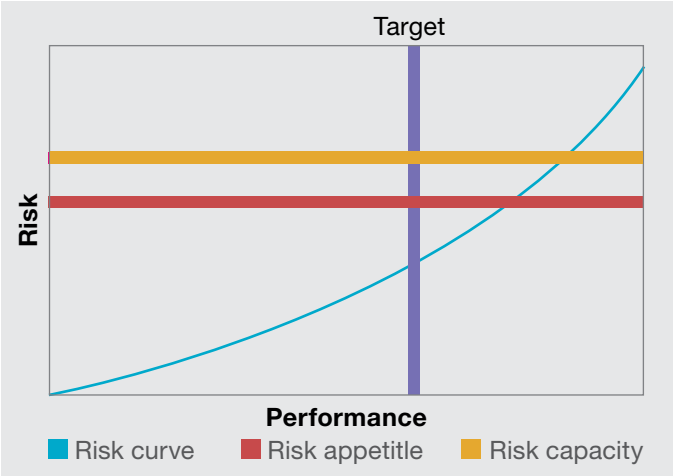


Figure D.3: Risk Profile with Risk Capacity



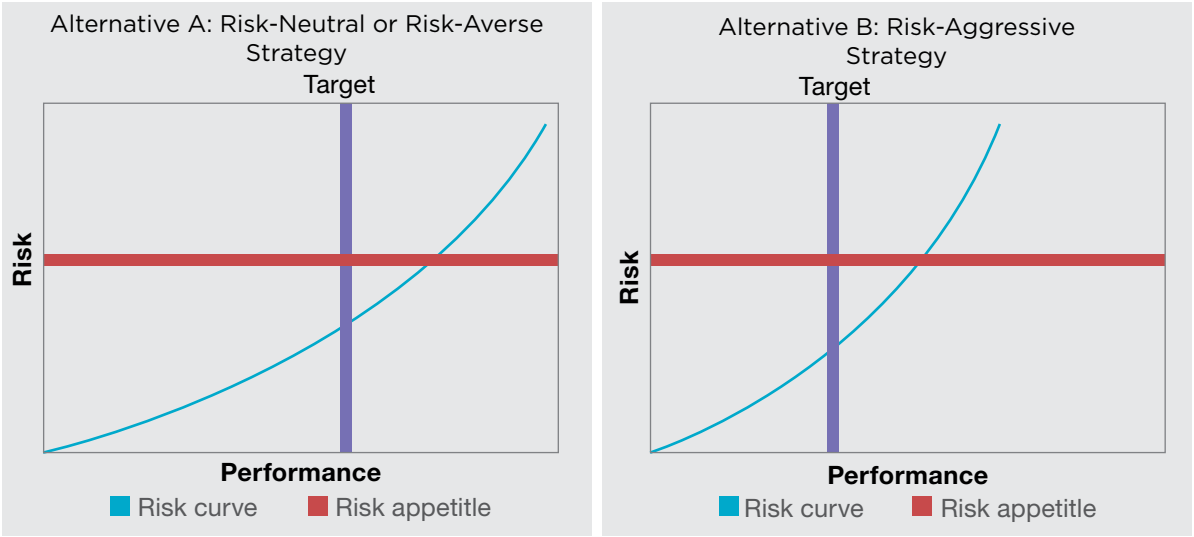
Using Risk Profiles to Consider Alternative Strategies

Organizations can develop profiles of potential risks as part of considering alternative strategies. For each strategy, an organization may prepare a risk profile that reflects the expected types and amount of risks. These risk profiles support the strategy selection process by highlighting differences in the expected risk for different strategies.

Figure D.4 illustrates how profiles can be compared. Alternative A shows a flatter curve, indicating that the entity faces less incremental risk as performance increases. That is, the intersection of the risk curve and risk appetite is farther to the right, indicating greater opportunity for performance before the entity exceeds appetite. Established entities operating in mature, stable markets or with stakeholders who expect lower risk profiles may seek strategies that resemble Alternative A.

Final Draft

Figure D.4: Risk Profiles of Alternative Strategies



Conversely, risk-taking entities such as start-ups or venture capitalists may explore strategies that are more typical of Alternative B. In this case, an entity would seek more aggressive performance in return for assuming greater risk.

Quantitative and qualitative techniques are used to develop the profile of potential risks and may be the same tools that are then used to support risk identification and assessment processes. This includes quantitative analysis and modeling where there is sufficient data. Where data is not available, more qualitative techniques may be employed.

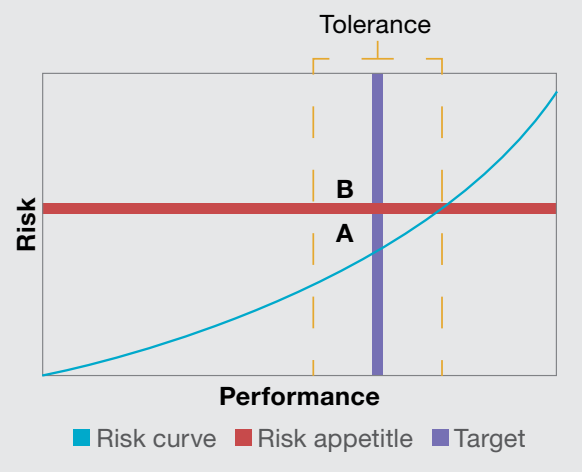
Considering Risk in Establishing Business Objectives and Setting Performance Targets

Once an organization selects a strategy, it carries out a similar analysis to establish business objectives. Organizations that are faced with alternative objectives seek to understand the shape and height of a curve for a potential business objective.

First, the organization sets a performance target for its business objectives. The performance target is determined in relation to the risk appetite and selected strategy. On a risk profile, the target demonstrates the desired performance and corresponding amount of risk (see Figure D.5).

Further, it illustrates the distance between the accepted amount of risk and risk appetite. The more aggressive the entity, the less will be the distance between the intersection of the performance target and the risk curve (Point A), and the intersection of performance target and risk appetite (Point B).

Figure D.5:
Risk Profile with Performance Targets



Final Draft

Final Draft

Using Risk Profiles to Demonstrate Acceptable Variation in Performance

The organization next determines the acceptable variation in performance on both sides of the target. This is illustrated in the figures by the dotted lines that run parallel to the performance target. The trailing and exceeding variances are set to reflect the risk appetite of the entity. There is no requirement that they be equidistant from the performance target. The closer the variances are set to the performance target, the less appetite for risk. However, by setting variations close to performance, management considers the trade-offs in the additional resources required to manage variability.

Identifying Risks in Performance

Organizations identify and assess the risks to business objectives and chosen strategy. Any potential risks that have been identified as part of the selection process provide a starting point for identifying and assessing risks in execution. This process yields a risk profile of actual risks for each business objective and overall strategy—one that either confirms the expected risks or one that indicates additional risks.

Additional risks may be identified for a number of reasons. The organization may have completed a more rigorous analysis after selecting a business objective, or may have gained access to more information, giving it more confidence in its understanding of the risk profile, or may have determined it needs to update the list of expected risks due to changes in the business context having occurred.

The outputs of the risk identification process, the risk universe, form the basis on which an organization is able to construct a more reliable risk profile.

Using Risk Profiles when Assessing Risk

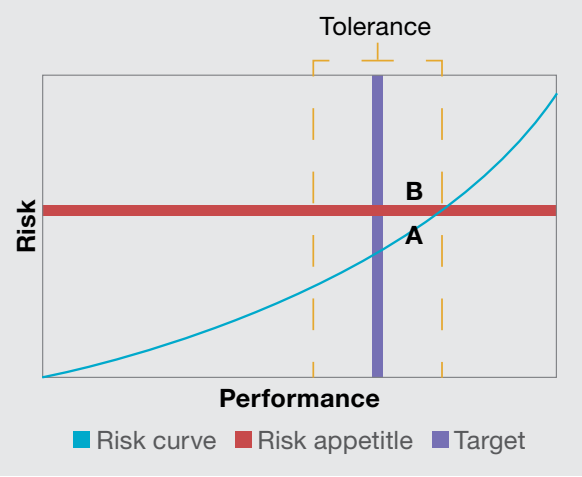
Risks identified and included in a risk profile are assessed in order to understand their severity to the achievement of an entity's strategy or business objectives. Management's assessment of risk severity can focus on different points of the risk profile for different purposes:

- To confirm that performance is within the acceptable variation in performance.
- To confirm that risk is within risk appetite.
- To compare the severity of a risk at various points of the curve.
- To assess the disruption point in the curve, at which the amount of risk has greatly exceeded the appetite of the entity and impacts its performance or the achievement of its strategy or business objectives

The risk profile in Figure D.6 depicts the amount of risk within an assumed time horizon. To incorporate time into the risk profile, management must define the performance target with reference to a time period.

In assessing the distance of the curve from the x-axis, management considers the aggregate amount of known (existing, emerging, and new risks) and unknown risks. The amount of unknown risk may be estimated with varying levels of

Figure D.6:
Assessing Risk Using a Risk Profile



confidence depending on the type of business objective, experience and knowledge of the organization, and available data. Where the number and amount of unknown risks is potentially large (e.g., developing new technology), the distance between the risk curve and the x-axis will typically be greater to indicate greater risk. For business objectives in more mature environments with significant performance data, knowledge, and experience, the amount of unknown risk may be considered much less significant, and the distance between the risk curve and the x-axis will therefore be smaller. The distance of the curve from the x-axis also demonstrates how multiple risks impact the same business objective.

The organization may choose to use different assessment methods for different points of the risk curve. When focused on the acceptable variation in performance, analysis of risk data may be a suitable approach. When looking at the extreme sections of the curve, scenario analysis workshops may prove more effective in determining the height and shape of the curve.

As with considering alternative strategies and identifying risks, management uses quantitative and qualitative approaches, or a combination of both, to assess risks and develop a risk profile. Qualitative assessment is useful when risks do not lend themselves to quantification or when it is neither practicable nor cost effective to obtain sufficient data for quantification. For example, consider a reputable technology company that is contemplating launching a new product that is currently not commercially available. In developing a risk profile of the risk of launching the R&D of the new product, management relies on its own business knowledge and its engineers' expertise to determine the height and shape of the curve.

For risks that are more easily quantifiable, or where greater granularity or precision is required, a probability modeling approach is appropriate (e.g., calculating value at risk or cash flows at risk). For example, when the same technology company assesses the risk of maintaining operations in a foreign country, it employs modeling when plotting the curve to identify sufficient points outlining the severity of its foreign exchange exposure.

Using Risk Profiles when Prioritizing Risks

How organizations prioritize risks can affect the risk profile for a strategy or business objective. The following are examples of how the prioritization criteria (see Principle 14) are incorporated into the risk profile:

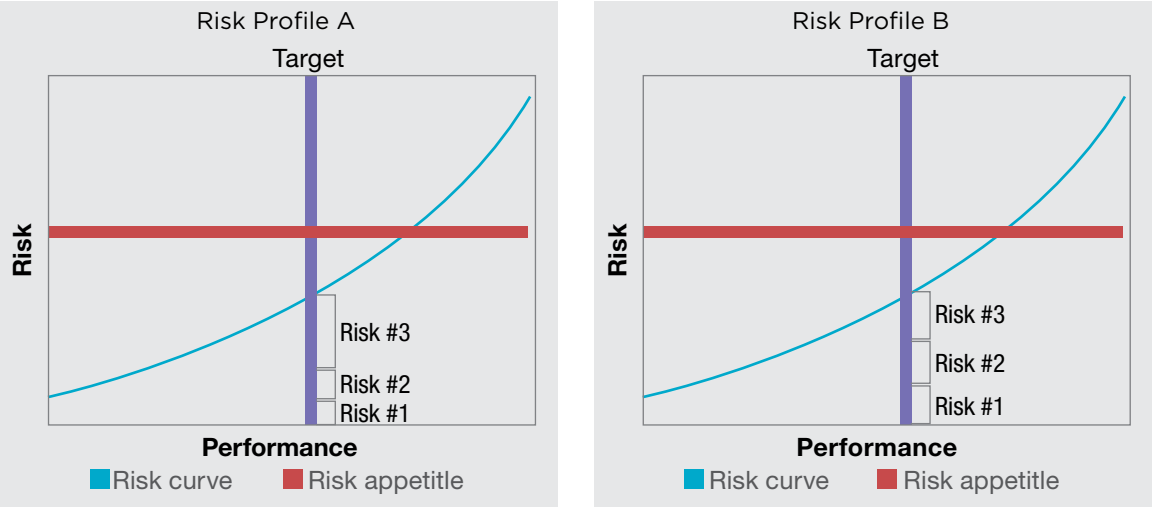
- *Adaptability* influences the height and shape of the risk curve reflecting the relative ease with which the organization can change and move along the curve.
- *Complexity* of a risk will typically shift the risk curve upwards to reflect greater risk.
- *Velocity* may affect the distance at which acceptable variation in performance is set from the target. (Note that the velocity of the risk also reflects the third dimension of time, and therefore is not reflected in the risk curve.)
- *Persistence*, not shown on the risk curve as it relates to a third dimension, may be reflected in a narrowing of the acceptable variation in performance as the entity acknowledges the sustained effect on performance.
- *Recovery*, the time taken to return to acceptable variation in performance, is considered part of persistence. How the entity recovers will shape the risk curve outside of the acceptable variation in performance and the relative ease with which the entity can move along the curve.

Many organizations choose to use severity as a prioritization criterion. For example, consider the risk profiles in Figure D.7. If an organization were asked to prioritize the risks in Risk Profile A compared to those in Risk Profile B, it may well select Risk #3 in Profile A as the most important because of its absolute severity (a risk-centric perspective). But if the organization were to view Risk Profile A from a business objective perspective, it would see that the entity is still well within its risk appetite for

Final Draft

the particular performance target. In fact, both Risk Profile A and B have the same severity of risk for their respective performance targets. Consequently, the severity of one risk (e.g., Risk #3 in Risk Profile A) should not be the sole basis for prioritization relative to other risks.

Figure D.7: Using Risk Profiles to Compare Risks Impacting Objectives



Using Risk Profiles when Considering Risk Responses

Once the organization develops a risk profile, it can determine if additional risk responses are required. The height and shape of the risk curve can be impacted depending on the risk response chosen (see Principle 15):

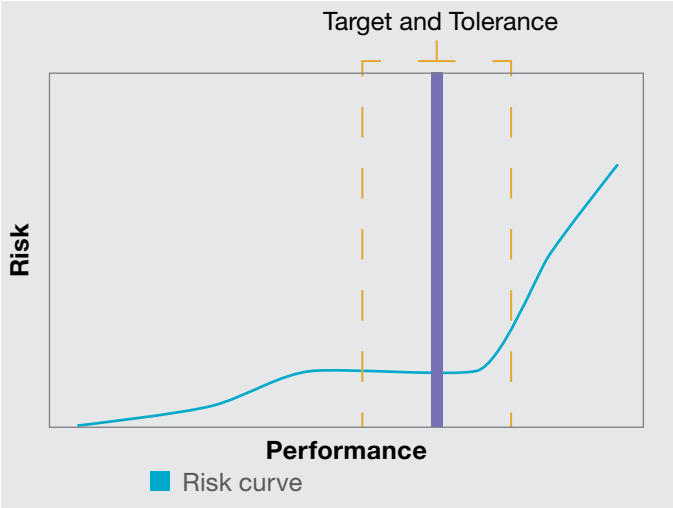
- *Accept:* No further action is taken to affect the severity of the risk and the risk profile remains the same. This response is appropriate when the performance of the entity and corresponding risk is below the risk appetite line and within the lines indicating acceptable variation in performance.
- *Avoid:* Action is taken to remove the risk, which may mean ceasing a product line, declining to expand to a new geographical market, or selling a division. Choosing avoidance suggests that the organization is not able to identify a response that would reduce the impact of the risk to an acceptable severity. Removing a risk will typically shift the curve downwards and/or to the left with the intent of having the target performance to the left of the intersection of the risk curve and the risk appetite.
- *Pursue:* Action is taken that accepts increased risk to achieve increased performance. This may involve adopting more aggressive growth strategies, expanding operations, or developing new products and services. When choosing to exploit risk, management understands the nature and extent of any changes required to achieve desired performance while not exceeding the target residual risk. Here the risk curve may not change but the target may be set higher, and therefore setting the target at a different point along the risk curve.
- *Reduce:* Action is taken to reduce the severity of the risk. This involves any of myriad everyday business decisions that reduce residual risk to the target residual risk profile and risk appetite. The intent of the risk response is to change the height and shape of the curve, or applicable sections of the curve, to remain within the risk appetite set for the entity. Alternatively, for risks that are already within the risk appetite, the reduce response may pertain to the reduction in variability of performance through the deployment of additional resources. The effective reduction of a risk would see a flattening of the risk curve for the sections impacted by the risk response.

Final Draft

- *Share:* Action is taken to reduce the severity of a risk by transferring or otherwise sharing a portion of the risk. Common techniques include outsourcing to specialist service providers, purchasing insurance products, and engaging in hedging transactions. As with the reduce response, sharing risk lowers residual risk in alignment with risk appetite. A section of the risk curve may change, although the entire risk curve likely shares similarities to one where risk has not been shared.
- *Review business objective:* The organization chooses to review and potentially revise the business objective given the severity of identified risks and acceptable variation in performance. This may occur when the other categories of risk responses do not represent desired courses of action for the entity.
- *Review strategy:* The organization chooses to review and potentially revise the strategy given the severity of identified risks and risk appetite of the entity. Similar to reviewing business objectives, this may occur when other categories of risk responses do not represent desired courses of action for the entity. Revisions to a strategy, or adoption of a new strategy, also require that a new risk profile be developed.

Figure D.8 shows how a risk profile changed after carrying out a risk response, such as entering into an insurance arrangement. For example, fruit farmers may purchase weather-related insurance for floods or storms that would result in their production levels dropping below a certain minimum. The risk curve for production levels flattens for the outcomes covered by insurance.

Figure D.8 Effect of Risk Response



Final Draft

Developing a Portfolio View

After selecting risk responses, management develops a composite view of residual risk (i.e., post-assessment and implementation of risk response). This composite view forms an entity-wide portfolio view of the risk that the entity faces.

While the portfolio view represents the view of risk at that level, management may choose to depict that view through a variety of lenses. Figures D.9 and D.10 illustrate two alternatives for viewing risk profile. The first, Figure D.9, illustrates a risk profile linked to strategy and entity objetives. The second, Figure D.10, illustrates the risk profile relating to the portfolio view of entity level onbjectives.

An organization may choose how to depict the portfolio depending on how performance is articulated and who is concerned. For instance, a chief financial officer may focus on a view that depicts the severity of risk in relation to financial performance. A chief operating officer may focus on a view that depicts the severity of risk in relation to operational performance. And the chief human resources officer may focus on a view that depicts the severity of risk in relation to culture and resource allocation. Yet, each of these views is based on one shared understanding of risk to business objectives.

Through the portfolio view, the organization identifies severe entity-level risks. Figure D.9 illustrates the portfolio view.

Figure D.9: Portfolio View Using Entity-Level Objectives



When preparing a portfolio view, the organization may also choose to develop a risk profile that provides added context on the portfolio view. Figure D.10 illustrates the risk profile of two entity-level objectives. The first graph illustrates how risk to the achievement of entity objective 1 (at the current level of performance) is within the both risk appetite and risk capacity (and shown as green in Figure D.9). The second graph illustrates how risk to the achievement of entity objective 2 is above the risk appetite, although still within risk capacity (Red in Figure D.9). These two perspectives are reflected above in Figure D.9.

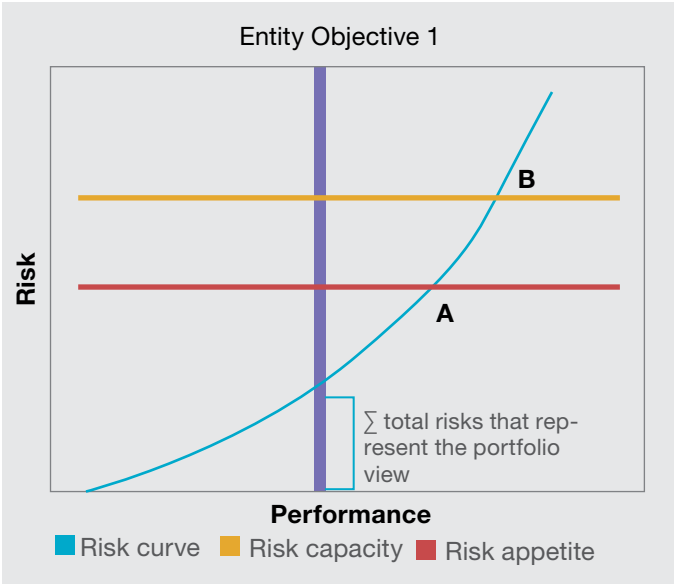
An organization will typically use both qualitative and quantitative techniques in developing this view. Qualitative techniques include scenario analysis and benchmarking. Quantitative techniques include regression modeling and other means of statistical analysis to determine the sensitivity of the portfolio to sudden or large changes. These changes may be represented as shifts in the risk curve or gradient.

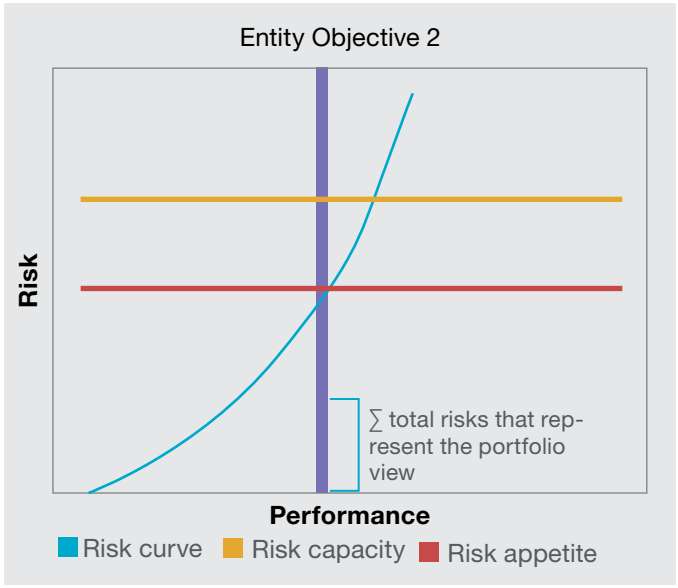
Final Draft

Analysis may also identify the point on the curve where change becomes a disruption to the performance of the entity. For example, using entity objective 1, an organization identifies that a drop of more than 25% in a specific index represents a disruptive change where the entity exceeds its risk appetite and affects the achievement of the strategy. This is represented at the point where the gradient of the curve steepens significantly (Point A). Further, the organization determines that a 50% drop would affect performance to the extent that the entity exceeds its risk capacity and threatens the viability of the entity. This is represented where the risk curve intersects the risk capacity line (Point B).

By using stress testing, scenario analysis, or other analytical exercises, an organization can avoid or more effectively respond to big surprises and losses. By analyzing the effect of hypothetical changes on the portfolio view, the organization identifies potential new, emerging, or changing risks and evaluates the adequacy of existing risk responses. The purpose of these exercises is for management to be able to assess the adaptive capacity of the entity. They also help management challenge the assumptions underpinning the selection of the entity's strategy and assessment of the risk profile.

Figure D.10:
Risk Profile relating to Entity Objective



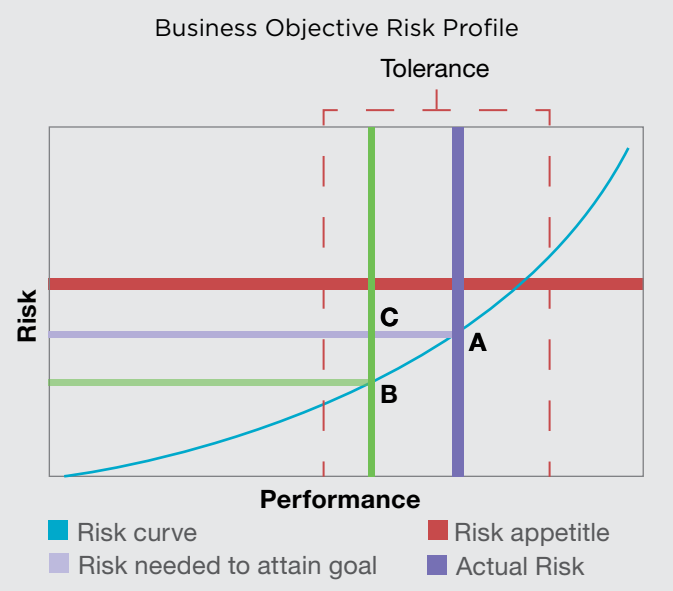


Final Draft

Monitoring Risk Management Performance

Organizations can use graphical representations to understand how risk is impacting performance. As shown in Figure D.11, management analyzes the risk profile to determine whether the current level of performance risk is greater, less than, or as expected compared to the risk assessment results. Additionally, management considers whether a change in performance has created new factors that influence the shape of the curve. Based on this analysis, management can take corrective action.

Figure D.11:
Using Risk Profiles to Monitor Performance



- Has the organization performed as expected and achieved its target? Using a risk profile, the organization reviews the performance set and determines whether targets were achieved or if variances occurred. Point B on the figure shows an organization that has not met its planned performance (Point A) but remains within acceptable variation.
- What risks are occurring that may be impacting performance? In reviewing performance, the organization observes which risks have occurred or are presently occurring. Monitoring also confirms whether risks were previously identified or whether new, emerging risks have occurred. That is, are the risks that were identified and assessed and that inform the shape and height of the risk curve consistent with what is being observed in practice?
- Was the entity taking enough risk to attain its target? Where an entity has failed to meet its target, the organization seeks to understand whether risks have occurred that are impacting the achievement of the target or whether insufficient risk was taken to support the achievement of the target. Given the actual performance of the entity in the figure, Point B also indicates that more risk could have been taken to attain its target.
- Was the estimate of risk accurate? In those instances where the risk was not assessed accurately, the organization seeks to understand why. In reviewing the assessment of severity, the organization challenges the understanding of the business context, the assumptions underpinning the initial assessment and whether new information has become available that may help refine the assessment results. Point C on the figure indicates where an entity has experienced more risk than anticipated for a given level of performance.

Given the results of the monitoring activities, the organization can determine the most appropriate course of action.

Final Draft