Committee of Sponsoring Organizations of the Treadway Commission

Enterprise Risk Management

Aligning Risk with Strategy and Performance

June 2016 edition

To submit comments on this Public Exposure Draft, please visit www.erm.coso.org. Responses are due by **September 15, 2016**. Respondents will be asked a series of questions. Those questions may be found on-line at www.erm.coso.org and in a separate document provided at the time of download. Respondents may upload letters through this site. Please do not send responses by fax.

Written comments on the exposure draft will become part of the public record and will be available on-line until **December 31, 2016**.

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

Committee of Sponsoring Organizations of the Treadway Commission

Board Members

PwC—Author

Principal Contributors

Miles E.A. Everson
Engagement Leader and US Advisory Leader
New York, USA

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

Frank J. Martens
Project Lead Director
Vancouver, Canada

Matthew Bagin
Director
Washington DC, USA

Hélène Katz
Director
New York, USA

Sallie Jo Perraglia
Manager
New York, USA

Kate T. Sylvis
Manager
McLean Virginia, USA

Kathleen Crader Zelnik
Manager
Washington DC, USA

Maria Grimshaw
Senior Associate
New York, USA

Advisory Council

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

Cynthia Armine-Klein
First Data Corporation
EVP Chief Control Officer

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

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

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 of Accountants
President and CEO

Vincent Tophoff
International Federation of Accountants
Senior Technical Manager

Table of Contents

Foreword

In keeping with its overall mission, the COSO Board commissioned and published in 2004 *Enterprise Risk Management—Integrated Framework*. Over the past decade, that publication has gained broad acceptance by organizations in their efforts to manage risk. However, also through that period, the complexity of risk has changed, new risks have emerged, and boards have enhanced their awareness and oversight of enterprise risk management while asking for improved risk reporting. This update to the 2004 publication addresses the evolution of enterprise risk management and the need for organizations to improve their approach to managing risk in today's business environment.

The new title, *Enterprise Risk Management—Aligning Risk with Strategy and Performance*, recognizes the increasing importance of the connection between strategy and entity performance. The updated content offers a perspective on current and evolving concepts and applications of enterprise risk management. As well, the second part of the publication, the Framework, accommodates different viewpoints and enhances strategies and decision-making. In short, this update:

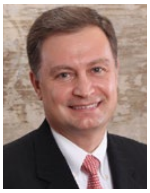
- Provides greater insight into the role of enterprise risk management when setting and executing strategy.
- Enhances alignment between performance and enterprise risk management.
- Accommodates expectations for governance and oversight.
- Recognizes the globalization of markets and operations and the need to apply a common, albeit tailored, approach across geographies.
- Presents new ways to view risk to setting and achieving objectives in the context of greater business complexity.
- Expands reporting to address expectations for greater stakeholder transparency.
- Accommodates evolving technologies and the growth of data analytics in supporting decision-making.

It also sets out core definitions, components, and principles, and provides direction for all levels of management involved in designing, implementing, and conducting enterprise risk management practices. As well, for those who are looking for an overview of these topics (boards of directors, chief executive officers, and other senior management), we have prepared an Executive Summary.

Readers may also wish to consult a complement to this publication, COSO's *Internal Control—Integrated Framework*. The two publications are distinct from each other and provide a different focus; neither supersedes the other. However, they do overlap. *Internal Control—Integrated Framework* encompasses internal control, which is referenced in part in this updated publication, and remains viable and suitable for designing, implementing, conducting, and assessing internal control and for consequent reporting.

The COSO Board would like to thank PwC for its significant contributions in developing this publication. Their full consideration of input provided by many stakeholders and their insight were instrumental in ensuring that the strengths of the original publication have been preserved, and that text has been clarified or expanded where it was deemed helpful to do so. The COSO Board and PwC together would also like to thank the Advisory Council and observers for their contributions in reviewing and providing feedback.

Robert B. Hirth Jr.
COSO Chair



Dennis L. Chesley
PwC Project Lead Partner
Global Risk Leader

Applying the Framework:
Putting It into Context

1. Introduction

Integrating enterprise risk management throughout an organization improves decision-making in governance, strategy, objective-setting, and day-to-day operations. It helps to enhance performance by more closely linking strategy and business objectives to both risk and opportunity. The diligence required to integrate enterprise risk management provides an entity with a clear path to creating, preserving, and realizing value.

1. A discussion of enterprise risk management[1] begins with this underlying premise: every entity—whether for-profit, not-for-profit, or governmental—exists to provide value for its stakeholders. This publication is built on a related premise: all entities face uncertainty in the pursuit of value. The concepts and principles of enterprise risk management set out in this publication are intended to apply to all entities regardless of legal structure, size, industry, or geography.
2. An "uncertainty" is generally understood to be something not completely known, or the condition of not being sure of something. Risk involves uncertainty and affects an organization's ability to achieve its strategy and business objectives. Therefore, one challenge for management is determining how much uncertainty—and therefore how much risk—the organization is prepared and able to accept. Effective enterprise risk management allows management to balance exposure against opportunity, with the goal of enhancing capabilities to create, preserve, and ultimately realize value.
3. Management has many choices in how it will apply enterprise risk management practices, and no one approach is better than another. However, readers who may be looking for information beyond a framework, or different practices that can be applied to integrate the concepts and principles into the entity, will find the appendices to this publication helpful.

Enterprise Risk Management Affects Value

4. The value of an entity is largely determined by the decisions that management makes—from overall strategy decisions through to day-to-day decisions. Those decisions can determine whether value is created, preserved, realized, or eroded.
   - Value is *created* when the value of resources deployed is less than the benefits derived from that deployment. These resources could be people, financial capital, technology, processes, and market presence (brand).
   - Value is *preserved* when the value of resources deployed in day-to-day operations sustain created benefits. For example, value is preserved with the delivery of superior products, service, and production capacity, which results in satisfied customers and stakeholders.

1 Defined terms are linked to Appendix A: Glossary of Terms when first used in the document.

- Value is *realized* when stakeholders derive benefits created by the entity. Benefits may be monetary or non-monetary.
- Value is *eroded* when management implements strategies that do not yield expected outcomes or fails to execute day-to-day tasks.

5. How value is created depends on the type of entity. For-profit entities create value by successfully implementing strategic decisions that balance market opportunities against the risks of pursuing those opportunities. Not-for-profit and governmental entities may create value by delivering goods and services that balance their opportunities to serve the broader community against any associated risks. Regardless of the type of entity, applying enterprise risk management practices creates trust and instills confidence with the stakeholders.

Enterprise Risk Management Affects Strategy

6. "Strategy" refers to an organization's plan to achieve its mission and vision, and to apply its core values. A well-defined strategy drives the efficient allocation of resources and effective decision-making. It also provides a road map for establishing business objectives.
7. Enterprise risk management does not create the entity's strategy, but it influences its development. An organization that integrates enterprise risk management into planning strategy provides management with the risk information it needs to consider alternative strategies and, ultimately, to adopt a specific strategy.

Enterprise Risk Management Is Linked to Business

8. Enterprise risk management is integrated with all other aspects of the business, including governance, strategy, performance management, and internal control. Specifically:
   - Governance and strategy form the broadest concept, encapsulating enterprise risk management, internal control, and performance management. Some aspects of governance fall outside of enterprise risk management (board member recruiting and evaluation; development of the entity's mission, vision, and core values).
   - Enterprise risk management incorporates aspects of internal control and intersects with performance management. Some aspects of enterprise risk management fall outside of both internal control and performance management (setting risk appetite and supporting the setting of strategy and objectives).
   - Performance management focuses on entity performance and deploying resources efficiently and effectively to achieve entity strategy and business objectives.

Performance Management

9. An organization sets out various actions to achieve, or exceed, its strategy and business objectives. Performance management is concerned with measuring those actions against predetermined targets (both short-term and long-term) and determining to what extent those targets are being achieved. However, because a variety of risks—both known and unknown—may affect an entity's performance, a variety of measures may be used:

- A financial measure, such as return on investments, revenue, or profitability.
- Operating performance, such as hours of operation, production volumes, or capacity percentages.
- Adherence to obligations, such as service-level agreements or regulatory compliance requirements.
- Rollout schedule for new products, such as having a new product launch every 180 days.
- A specific growth target, such as expanding market share in an emerging market.
- Delivery of agreed-upon level of service to a designated population on time and within budget.

10. An entity's overall performance can be enhanced by integrating enterprise risk management into day-to-day operations and more closely linking business objectives to risk and opportunity.

Internal Control

11. "Internal control" is best described as a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance that objectives relating to operations, compliance, and reporting will be achieved. Internal control helps the organization to understand the risks to achieving those objectives and how to manage risks to an acceptable level. Having a system of internal control allows management to stay focused on the entity's operations and the pursuit of its performance targets while operating within the parameters of relevant laws and regulations.
12. COSO's publication *Internal Control—Integrated Framework* is intended to help management better manage the risks associated with achieving their objectives, and to enable a board of directors to oversee internal control. To avoid redundancy, some aspects of internal control that are common to both this publication and *Internal Control—Integrated Framework* have not been repeated here (e.g., assessment of fraud risk relating to financial reporting objectives, control activities relating to compliance objectives, the need to conduct ongoing and separate evaluations relating to operations objectives). However, other aspects of internal control are further developed in the Framework[2] section (e.g., governance aspects of enterprise risk management). Please review *Internal Control—Integrated Framework*[3] as part of applying the Framework in this publication.

2 In this document, the term "Framework" refers collectively to the five components introduced in Chapter 5 and covered individually in Chapters 6 through 10.

3 *Internal Control—Integrated Framework* can be obtained through www.coso.org.

Benefits of Enterprise Risk Management

13. An organization needs to be able to identify challenges that lie ahead and adapt to meet those challenges. It must engage in decision-making with an awareness of both the opportunities for creating value and the risks that challenge the achievement of value. In short, it must integrate enterprise risk management practices with strategy-setting and performance management, and in doing so it will realize many benefits related to value.
14. Benefits include the ability to:

    - *Increase the range of opportunities*: By considering all reasonable possibilities—both positive and negative aspects of risk—management can identify opportunities for the entity and unique challenges associated with current opportunities. For example, when the managers of a food company considered potential risks likely to affect the business objective of sustainable revenue growth, they determined that the company's primary consumers were becoming increasingly health conscious and changing their diet. This change indicated an uncertainty: a potential decline in future demand for the company's current products. In response, management identified ways to develop new products and improve existing ones, which allowed the company to maintain revenue from existing customers (preserving value) and to create additional revenue by appealing to a broader consumer base (creating value).
    - *Identify and manage entity-wide risks*: Every entity faces myriad risks that can affect many parts of the entity. Sometimes a risk can originate in one part of the entity but impact a different part. Management must identify and manage these entity-wide risks to sustain and improve performance. For example, when a bank realized that it faced a variety of risks in trading activities, management responded by developing a system to analyze internal transaction and market information that was supported by relevant external information. The system provided an aggregate view of risks across all trading activities, allowing drill-down capability to departments, customers, and traders. It also allowed the bank to quantify the relative risks. The system met the entity's enterprise risk management requirements and allowed the bank to bring together previously disparate data to respond more effectively to risks.
    - *Reduce surprises and losses*: Enterprise risk management allows organizations to improve their ability to identify potential risks and establish appropriate responses, reducing surprises and related costs or losses. For example, a manufacturing company that provides just-in-time parts to customers for use in production risks penalties for failing to deliver on time. In response to this risk, the company assessed its internal shipping processes by reviewing factors such as time of day for deliveries, typical delivery routes, and unscheduled repairs on the delivery fleet. It used the findings to set maintenance schedules for its delivery fleet, schedule deliveries outside of rush periods, and devise alternatives to key routes. Recognizing that not all traffic delays can be avoided, it also developed protocols to warn clients of potential delays. In this case, performance was improved by management influencing risk within its ability (production and scheduling) and adapting to risks beyond its direct influence (traffic delays).
    - *Reduce performance variability*: For some entities, the challenge is less about surprises and losses, and more about performance variability. Performing ahead of schedule or beyond expectations may cause as much concern as performing below expectations. For instance, within a public transportation system, riders will be just as annoyed when a bus or train departs 10 minutes early as when it is 10 minutes late: both can cause riders to miss connections. To manage such variability, transit schedulers build natural pauses into the schedule. Drivers wait at designated stops until a set time, regardless of when they arrive. Doing so helps to smooth out variability in travel times and improve overall performance and rider views of the transit system. Enterprise risk management allows organizations to anticipate the risks that would impact performance and enable them to take action to minimize disruption.

- *Improve resource deployment*: Obtaining robust information on risk allows management to assess overall resource needs and enhance resource allocation. For example, a downstream gas distribution company recognized that its aging infrastructure increased the risk of a gas leak occurring. By looking at trends in gas leak–related data, the organization was able to assess the risk across its distribution network. Management subsequently developed a plan to replace worn-out infrastructure and repair those sections that had remaining useful life. This approach allowed the company to maintain the integrity of the infrastructure while allocating the need for significant additional resources over a longer period of time.

15. Keep in mind that the benefits of integrating enterprise risk management with strategy-setting and performance management will vary by entity. There is no one-size-fits-all approach available for all entities. However, implementing enterprise risk management will generally help an organization achieve its performance and profitability targets and prevent or reduce the loss of resources.

Enterprise Risk Management and the Capacity to Adapt, Survive, and Prosper

16. Every entity sets out to achieve its strategy and business objectives, doing so in an environment of change. Market globalization, technological breakthroughs, mergers and acquisitions, fluctuating capital markets, competition, political instability, workforce capabilities, and regulation, among other things, make it difficult to know all possible risks to that strategy and business objectives.
17. Because risk is always present and always changing, pursuing goals can be difficult. While it may not be possible for organizations to manage all potential outcomes of a risk, they can improve how they adapt to changing circumstances. This is sometimes referred to as organizational sustainability.[4] The Framework (see Chapters 6 through 10) incorporates this concept in the broad context of creating, preserving, and realizing value.
18. Enterprise risk management focuses on managing risks to reduce the likelihood that an event will occur, and on managing the impact when one does occur. "Managing the impact" may require an organization to adapt as circumstances dictate. In some extreme cases, this may include implementing a crisis management plan.
19. Consider, for instance, a cruise ship operator that is concerned with the potential of viral outbreaks occurring while its ships are at sea. A cruise ship does not have the capability to quarantine passengers during an outbreak, but it can carry out procedures to minimize the spread of germs. However, despite installing hand-sanitizing stations throughout the ship, providing laundry facilities, and daily disinfecting handrails, washrooms, and other common areas, viral outbreaks still can and do occur. The organization responds by implementing specific protocols. First, routine on-board cleaning and sanitizing is escalated. Once the ship is in port, all passengers are required to disembark to allow specially trained staff to disinfect the entire ship. Afterwards, cleaning protocols are updated based on the strain of virus found. The next departing cruise is delayed until all cleaning protocols are addressed. In most instances, the delay is less than 48 hours. By having strong enterprise risk management capabilities in place to immediately respond and adapt to each unique situation, the company is able to minimize the impact while maintaining passenger confidence in the cruise line.
20. Sometimes an organization is not able to return to normal operations in the near term when an event occurs. In these cases, the organization must adopt a longer-term solution. For instance, consider a cruise ship that is disabled at sea by a fire. Unlike the scenario of a viral outbreak affecting only a few passengers, the fire impacts all passengers. There may be an immediate need for

4 Other terms used are "resilience," "agility," "corporate social responsibility," "corporate citizenship," "and stewardship."

medical assistance, food, water, and shelter, or even a call to off-load all ship passengers. Because ships are seldom in the same place, common crisis response planning may be less effective as each location and type of incident can present different challenges. However, by scheduling its fleet location and staggering departure schedules, the company can maintain a routing where ships are always within 24 hours of port or another cruise ship. This overlap allows the company to rapidly redeploy ships and crews to assist in an emergency.

21. Management will be in a better position if it takes time to anticipate what may transpire—the probable, the possible, and the unlikely. The capacity to adapt to change makes an organization more resilient and better able to evolve in the face of marketplace and resource constraints. This capacity may also give management the confidence to increase the amount of risk the organization is willing to accept and, ultimately, to accelerate growth and increase value.

2. Understanding the Terms: Risk and Enterprise Risk Management

Defining Risk and Uncertainty

22. There is risk in not knowing how an entity's strategy and business objectives may be affected by potential events. The risk of an event occurring (or not), creates uncertainty. In business,[5] uncertainty exists whenever an entity sets out to achieve future strategies and business objectives. In this context, risk is defined as:

    The possibility that events will occur and affect the achievement of strategy and business objectives.

23. The box on this page contains terms that expand on and support the definition of risk. The Framework (Chapters 6 through 10) emphasizes that risk relates to the potential for events, often considered in terms of severity. In some instances, the risk may relate to the anticipation of an event that does not occur.

- **Event:** An occurrence or set of occurrences.
- **Uncertainty:** The state of not knowing how potential events may or may not manifest.
- **Severity:** A measurement of considerations such as the likelihood and impacts of events or the time it takes to recover from events.

24. In the context of risk, events are more than routine transactions; they are broader business matters such as changes in the governance and operating model, geopolitical and social influences, and contracting negotiations, among other things. Some events are readily discernable—a change in interest rates, a competitor launching a new product, or a cyber attack. Others are less evident, particularly when multiple small events combine to create a trend or condition. For instance, it may be difficult to identify specific events related to global warming, yet that condition is generally accepted as occurring. In some cases, organizations may not even know or be able to identify what events may occur.

25. Organizations commonly focus on those risks that may result in a negative outcome, such as damage from a fire, losing a key customer, or a new competitor emerging. However, events can also have positive outcomes, and these must also be considered. As well, events that are beneficial to the achievement of one objective may at the same time pose a challenge to the achievement of other objectives. For example, a product launch with higher-than-forecast demand introduces a risk to the supply chain management, which may result in unsatisfied customers if the company cannot supply the product.

26. Some risks have minimal impact on an entity, and others have a larger impact. A role of enterprise risk management is to identify and focus on those risks that may prevent value from being created, preserved, realized, or that may erode existing value. Enterprise risk management helps the organization pursue potential opportunities associated with risk.

5 "Business" is a broad term that can encompass a wide variety of operating practices including for-profit, not-for-profit, and governmental entities.

Defining Enterprise Risk Management

27. Enterprise risk management is defined here as:

    The culture, capabilities, and practices, integrated with strategy-setting and its execution, that organizations rely on to manage risk in creating, preserving, and realizing value.

28. A more in-depth look at the definition of enterprise risk management emphasizes its focus on managing risk through:

    - Recognizing culture and capabilities.
    - Applying practices.
    - Integrating with strategy-setting and its execution.
    - Managing risk to strategy and business objectives.
    - Linking to creating, preserving, and realizing value.

Recognizing Culture and Capabilities

29. Culture is a key aspect of enterprise risk management. Culture is developed and shaped by the people at all levels of an entity by what they say and do. It is people who establish the entity's mission, strategy, and business objectives, and put enterprise risk management practices in place. Similarly, enterprise risk management affects people's actions. Each person has a unique point of reference, which influences how he or she identifies, assesses, and responds to risk. Enterprise risk management helps people understand risk in the context of the entity's strategy and business objectives.

30. Similarly, enterprise risk management provides a core capability to an organization. Organizations pursue various competitive advantages to create value for the entity. Enterprise risk management helps the organization develop the skills needed to execute the entity's mission and vision and to anticipate the challenges that may impede organizational success. An organization that has the capacity to adapt to change is more resilient and better able to evolve in the face of marketplace and resource constraints.

Applying Practices

31. Enterprise risk management is not static, nor is it an adjunct to a business. Rather, it is continual, being applied to the entire scope of activities as well as special projects and new initiatives. It is part of management decisions at all levels of the entity.

32. The practices used in enterprise risk management are applied from the highest levels of an entity and flow down through divisions, business units, and functions. The practices are intended to help people within the entity better understand its strategy, what business objectives have been set, what risks exist, what the acceptable amount of risk is, how risk impacts performance, and how to manage risk. In turn, this understanding supports decision-making at all levels and helps to reduce organizational bias.

Integrating with Strategy-Setting and Its Execution

33. An organization sets strategies that align with and support its mission and vision. It also sets business objectives that flow from the strategy, cascading to the entity's business units, divisions, and functions. At the highest level, enterprise risk management is integrated with strategy-setting, with management considering the implications of each strategy to the entity's risk profile. Management specifically considers any new opportunities that arise through innovation and emerging pursuits.

34. But enterprise risk management doesn't stop there; it continues in the day-to-day tasks of the entity, and in so doing may realize significant benefits. An organization that integrates enterprise risk management into daily tasks is more likely to have lower costs compared with one that "layers on" enterprise risk management procedures. In a highly competitive marketplace, such cost savings can be crucial to a business's success. As well, by building enterprise risk management into the fabric of the entity, management is likely to identify new opportunities to grow the business.
35. Enterprise risk management integrates with other management processes as well. Specific actions are needed for specific tasks, such as business planning, operations, and financial management. An organization considering credit and currency risks, for example, may need to develop models and capture large amounts of data necessary for analytics. By integrating these actions with an entity's operating activities, enterprise risk management can become more effective.

Managing Risk to Strategy and Business Objectives

36. Enterprise risk management is integral to achieving strategy and business objectives. Well-designed enterprise risk management practices provide management and the board of directors with a reasonable expectation that they can achieve the overall strategy and business objectives of the entity. Having a reasonable expectation means that the amount of uncertainty of achieving strategy and business objectives is appropriate for that entity, recognizing that no one can predict risk with precision.
37. Even entities with strong enterprise risk management practices can experience unforeseen challenges, including operating failure. However, robust enterprise risk management practices will increase management's confidence in the entity's ability to achieve its strategy and business objectives.

Linking to Creating, Preserving, and Realizing Value

38. An organization must manage risk to strategy and business objectives in relation to its risk appetite—that is, the types and amount of risk, on a broad level, it is willing to accept in its pursuit of value. Specifically, risk appetite provides guidance on the practices an organization is encouraged to pursue or not pursue. Risk appetite sets the range of appropriate practices rather than specifying a limit. Different strategies will expose an entity to different risks or different amounts of similar risks.
39. Enterprise risk management helps management select a strategy that aligns anticipated value creation with the entity's risk appetite and its capabilities for managing risk more often and more consistently over time. Managing risk within risk appetite enhances an organization's ability to create, preserve, and realize value.

3. Enterprise Risk Management and Strategy

40. When enterprise risk management and strategy-setting are integrated, an organization is better positioned to understand:

    - How mission, vision, and core values form the initial expression of acceptable types and amount of risk for consideration when setting strategy.
    - The possibility of strategies and business objectives not aligning with the mission, vision, and core values.
    - The types and amount of risk the organization potentially exposes itself to from the strategy that has been chosen.
    - The types and amount of risk to executing its strategy and achieving business objectives.

41. Figure 3.1 illustrates strategy being set in the context of mission, vision, and core values, and a driver of an entity's overall direction and performance.

Figure 3.1: Strategy in Context

Mission, Vision, and Core Values

42. An entity's mission, vision, and core values[6] define what it strives to be and how it wants to conduct business. They communicate to stakeholders the purpose of the entity. For most entities, mission, vision, and core values remain stable over time, and during strategy planning, they are typically reaffirmed. Yet, the mission, vision, and core values may evolve as the

- **Mission:** The entity's core purpose, which establishes what it wants to accomplish and why it exists.
- **Vision:** The entity's aspirations for its future state or what the organization aims to achieve over time.
- **Core Values:** The entity's beliefs and ideals about what is good or bad, acceptable or unacceptable, which influence the behavior of the organization.

6 Note that some entities use different terms, such as "credo," "purpose," "philosophy," "fundamental beliefs," and "policies." Regardless of the terminology used, the concepts underlying mission, vision, and core values provide a structure for communicating throughout the entity.

expectations of stakeholders change. For example, a new executive management team may present different ideas for the mission in order to add value to the entity.

43. In the Framework (Chapters 6 through 10), mission and vision are considered in the context of an organization setting and carrying out its strategy and business objectives. Core values are considered in the context of the culture the entity wishes to embrace.

The Importance of Aligning Strategy

44. Both mission and vision provide a view from up high of the acceptable types and amount of risk for the entity. They help the organization to establish boundaries and focus on how decisions may affect strategy. An organization that understands its mission and vision can set strategies that will yield the desired risk profile.

45. Consider the statements from a healthcare provider in Figure 3.2.

Figure 3.2: Sample Mission, Vision, and Core Values

Mission: To improve the health of the people we serve by providing high-quality care, a comprehensive range of services, and convenient and timely access with exceptional patient service and compassion.

Vision: Our hospital will be the healthcare provider of choice for physicians and patients, and be known for providing unparalleled quality, delivering celebrated service, and being a terrific place to practice medicine.

Core Values: Our values serve as the foundation for everything we think, say, and do. We will treat our physicians, patients, and our colleagues with respect, honesty, compassion, and accountability.

46. These statements guide the organization in determining the types and amount of risk it is likely to encounter and accept. For instance, the organization would consider the risks associated with providing high-quality care (mission), providing convenient and timely access (mission), and being a terrific place to practice medicine (vision). Considering its high regard for quality, service, and breadth of skill, the organization is likely to seek a strategy that has a lower-risk profile relating to quality of care and patient service. This may mean offering in-patient and/or out-patient services, but not a primary on-line presence. On the other hand, if the organization had stated its mission in terms of innovation in patient care approaches or advanced delivery channels, it may have adopted a strategy with a different risk profile.

47. In short, an entity's strategy should align with—or support—the entity's mission, vision, and core values. If the strategy is not aligned, the organization's ability to realize its mission and vision may be significantly reduced. This can happen even if the (mis)aligned strategy is successfully executed. For instance, in the case of the healthcare company described in Figure 3.2, had it adopted a strategy of focusing on being the best provider of specialist services in select areas, it would have diminished the probability of successfully providing a comprehensive range of patient services.

48. Integrating enterprise risk management can help an entity avoid misaligning a strategy. It can provide an organization with insight to ensure that the strategy it chooses supports the entity's broader mission and vision for management and board consideration.

Evaluating the Chosen Strategy

49. Enterprise risk management does not create the entity's strategy, but it informs the organization on risks associated with alternative strategies considered and, ultimately, with the adopted strategy. The organization needs to evaluate how the chosen strategy could affect the entity's risk profile, specifically the types and amount of risk the organization is potentially exposed to.
50. When evaluating potential risks that may arise from strategy, management also considers critical assumptions they have made that underlie the chosen strategy. Enterprise risk management provides valuable insight into how sensitive changes to assumptions are; that is, whether they would have little or great effect on achieving the strategy.
51. Consider again the mission and vision of the healthcare provider discussed earlier, and how they cascade into the entity's strategy (Figure 3.3).

Figure 3.3: Sample Strategy Statement

Our Strategy:

- Maximize value for our patients by improving quality across a diverse spectrum of services
- Curtail trends in increasing costs.
- Integrate operating efficiency and cost-management initiatives.
- Align physicians and clinical integration.
- Leverage clinical program innovation.
- Grow strategic partnerships.
- Manage patient service delivery, and reduce wait times where practical.

52. Using the statement shown in Figure 3.3, the organization can consider what risks may result from the strategy chosen. For instance, risks relating to medical innovation may be more pronounced, risks to the ability to provide high-quality care may elevate in the wake of cost-management initiatives, and risks relating to managing new partnerships may be new to the organization. These and many other risks result from the choice of strategy. There remains the question of whether the entity is likely to achieve its mission and vision with this strategy, or whether there is an elevated risk to achieving the goals set.

Risk to Executing the Strategy

53. There is always risk to executing strategy, which every organization must consider. Here, the focus is on understanding the strategy set out and what risks there are to its relevance and viability. Sometimes the risks become important enough that an organization may wish to revisit its strategy and consider revising it or selecting one with a more suitable risk profile.
54. The risk to executing strategy may also be viewed through the lens of business objectives. Objectives are the basis upon which risks are identified and assessed. An organization can use a variety of techniques to assess risks, but wherever possible, it should strive to use some kind of measure, and then use the same or similar units of measure for each objective. Doing so will help to align the severity of the risk with established performance measures.

55. In assessing risk to executing the strategy, management specifies business objectives—such as financial performance, customer satisfaction, learning and growth, and compliance—and assigns these to different parts of the entity. For instance, in the example introduced in Figure 3.2, the healthcare company has a business objective of high-quality patient care. Therefore, the organization considers risks relating to employee capability, medical care and treatment, healthcare legislation reform, and access to electronic health records, among others.
56. The entity's governance and operating models can also influence the organization's ability to identify, assess, and respond to risks to the achievement of strategy. Regardless of the models adopted, an entity must understand this influence.

Governance and Operating Models

57. An entity's governance model defines and establishes authority, responsibility, and accountability. It aligns the roles and responsibilities to the operating model at all levels—from the board of directors to management, to divisions, to operating units, and to functions. Enterprise risk management helps to inform all levels of potential risks to strategy and how the organization is managing them.
58. An operating model describes how management organizes and executes its day-to-day operations. It is typically aligned with the legal structure and management structure. Through the operating model, personnel are responsible for developing and implementing practices to manage risk and stay aligned with the core values of the entity. In this way, an operating model contributes to managing risk to the strategy.

Legal Structure

59. How an entity is structured legally influences how it operates, and different legal structures may be more or less suitable depending on a variety of factors, including size of the entity and any relevant regulatory, taxation, or shareholder structures. A small entity is likely to operate as a single legal entity. Large entities may consist of several distinct legal entities, in which case risks may be segregated if they do not aggregate across legal models.

Management Structure

60. The management structure sets out the reporting lines, roles, and responsibilities for ongoing management and operation of the business. Under the management structure, reporting usually transcends the legal structures of the entity. For example, a company that has three separate legal divisions reports as one consolidated company.
61. Factors that may influence the structure of management include regulatory requirements, tax implications, reporting requirements, workforce availability and mobility, geographic concentrations and focus, market competitiveness, capital availability, and the complexity of products or services. For example, a multinational bank may have different core products and services, such as mortgages, retail banking, and credit cards. The bank offers these core products across legal entities. Another entity may choose to structure itself based on geographic territory. For example, a large global beverage company may operate and report by its territories of North America, Latin America, Europe, Africa, and Asia Pacific.

Managing Risks through the Value Chain

62. The discussion above focuses on managing risks to executing strategy through the business model. But some organizations will view enterprise risk management through the lens of the value chain model.[7] Traditionally, in this model, an organization analyzes where and how it can create value to gain a competitive advantage. Organizations may create value through different parts of the value chain. One entity may create value by having superior distribution capabilities, another through marketing, and another through its ability to repeatedly deliver innovative products.

63. Enterprise risk management may be applied across a value chain. In this case, entities analyze how risk can affect the achievement of strategy and business objectives across the entire value chain. Such an analysis allows organizations to determine the capabilities needed to execute the entity's strategy, and ultimately create, preserve, and realize value.

7 One such model was popularized by Michael Porter, a leading authority on competitive strategy, in his 1985 book *Competitive Advantage*.

4. Considering Risk and Entity Performance

Risk and Uncertainty

64. "Performance" describes how actions are carried out as measured against a pre-set target. There is always risk associated with a target of performance.

65. Whatever the level of entity performance, uncertainty exists. Or, stated conversely, the amount of uncertainty that exists anticipates a particular amount of risk to performance. For example, large-scale agriculture producers will have a certain amount of uncertainty about their ability to produce the volumes required to satisfy customer demands and meet profitability targets. Similarly, airlines will have a certain amount of uncertainty about their ability to operate all flights on their schedule. Yet, airline companies may be less uncertain that they can operate 90% or even 80% of their scheduled flights. In both of these examples, there is an amount of uncertainty associated with each level of performance—production volume and flight operation.

66. Risk is often depicted graphically as a single point intersecting the level of performance. However, this does not illustrate how the amount of risk may change, thereby affecting performance of an entity. And if the level of desired performance changes, the severity of a risk will likely change as well.

Understanding the Risk Profile

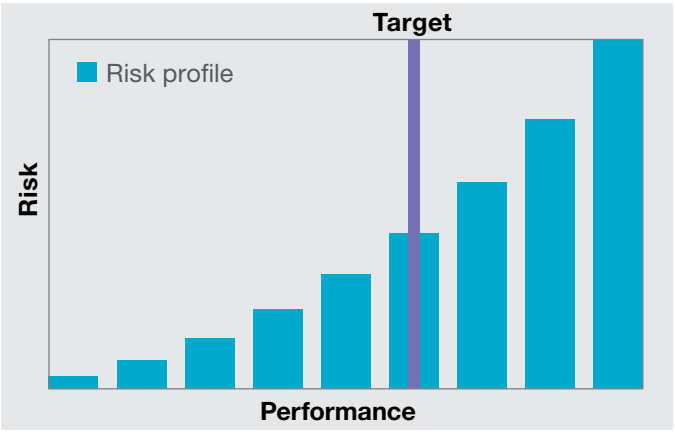
67. An entity's risk profile provides a composite view of the risk at a particular level of the entity or aspect of the business model. This composite view allows management to consider the type, severity, and interdependencies of risks, and how they may affect performance relative to strategy and business objectives.

68. This relationship between risk and performance is rarely linear and one-to-one. Incremental changes in performance targets do not always result in corresponding changes in risk, and therefore the single-point illustration is not always helpful. A more realistic representation of risk profile, sometimes depicted graphically, illustrates the aggregate amount of risk associated with different levels of performance. Such a representation considers risk as a continuum of potential outcomes along which the organization must balance the amount of risk to the entity and its desired performance.

69. There are several methods for depicting a risk profile. The Framework (Chapters 6 through 10) uses one approach, shown here, to illustrate the relationship between various aspects of enterprise risk management.

70. In Figure 4.1, each bar represents the risk profile for a specific point of performance. The vertical target line depicts the level of performance chosen by the organization as part of strategy-setting, which is communicated through a business objective and target.

Figure 4.1: A Risk Profile



71. Risk profiles that trend upwards, as shown in Figure 4.1, are typical of business objectives related to:

    - *Oil and gas exploration*: As exploration efforts for new oil and gas reserves target increasingly remote and inaccessible areas, oil and gas companies likely face greater amounts of risk in an effort to locate resources.
    - *Mining extraction*: As the number of mines grows to meet global demand, or the mining operations become more complex, an international mining company is likely to see increases in the amount of risk to its operations around the globe.
    - *Recruitment of specialist resources*: As entities grow, the risks associated with attracting and retaining expertise and experience in its workforce increases.
    - *Funding for capital works and improvements*: In illiquid markets, or where consumer confidence is low, the amount of risk associated with a firm's ability to secure funding for capital works, projects, or initiatives increases.

72. There is, however, no one universal risk profile shape or trend. Every entity's risk profile will be different depending on its unique strategy and business objectives. Organizations can use their risk profiles to better understand and discuss the intrinsic relationship between risk and performance.

Expressing Risk Appetite

73. Risk appetite is integral to enterprise risk management. It guides decisions on the types and amount of risk an organization is willing to accept in its pursuit of value. The first expression of risk appetite is an entity's mission and vision.[8] Risk appetite is not static; it may change over time in line with changing capabilities for managing risk. Further, the process of selecting strategy and developing risk appetite is not linear, with one always preceding the other. Many organizations develop strategy and risk appetite in parallel, refining each throughout the strategy-setting process.

74. Nor is there a universal risk appetite that applies to all entities. Some entities consider risk appetite in qualitative terms while others prefer quantitative terms, often focusing on balancing growth, return, and risk. Whatever the approach for describing risk appetite, it should reflect the entity's culture. The best approach for an entity is one that aligns with the analysis used to assess risk in general, whether that is qualitative or quantitative. Developing the risk appetite statements is an exercise in finding a compromise between risks and opportunities.

75. It is up to management to develop the risk appetite statement. Some organizations may consider a general term like "low appetite" clear, while others may find such a statement too vague and difficult to communicate and implement throughout the entity. It is common for risk appetite statements to become more precise as organizations become more experienced in enterprise risk management. It is also common for organizations to develop a series of "sub-level" expressions cascading from the overarching risk appetite statement. These lower-level statements offer more precision, and use terms such as "targets," "ranges," "floors," or "ceilings." These statements may consist of:

    - *Strategic parameters*: Considering matters such as new products to pursue or avoid, the investment for capital expenditures, and merger and acquisition activity.
    - *Financial parameters*: Considering matters such as the maximum acceptable variation in financial performance, return on assets or risk-adjusted return on capital, target debt rating, and target debt/equity ratio.
    - *Operating parameters*: Considering matters such as capacity management, environmental requirements, safety targets, quality targets, and customer concentrations.

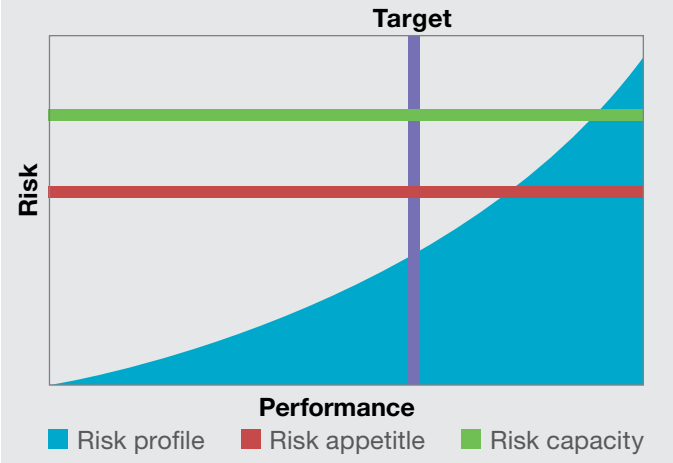
8 Risk appetite is discussed further in the Framework under Principle 8: Defines Risk Appetite.

76. Taken together, these considerations help frame the entity's risk appetite and provide greater precision than a single, higher-level statement.

77. Figure 4.2 depicts the risk profile as a solid area (in blue), filling in the space across the performance axis from the individual risk profile bars. A line showing risk appetite has also been added.

78. While risk appetite is introduced here, the Framework sets out numerous instances where risk appetite is applied as part of enterprise risk management. Some of the more important applications of risk appetite are:

Figure 4.2: Risk Profile Showing Risk Appetite and Risk Capacity



- Its help in aligning the acceptable amount of risk with the organization's capacity to manage risk.
- Its relevance when setting strategy and business objectives, helping management consider whether performance targets are aligned with acceptable amount of risk.
- Its relevance and alignment with risk capacity.
- Its use in evaluating aggregated risk of the portfolio view.

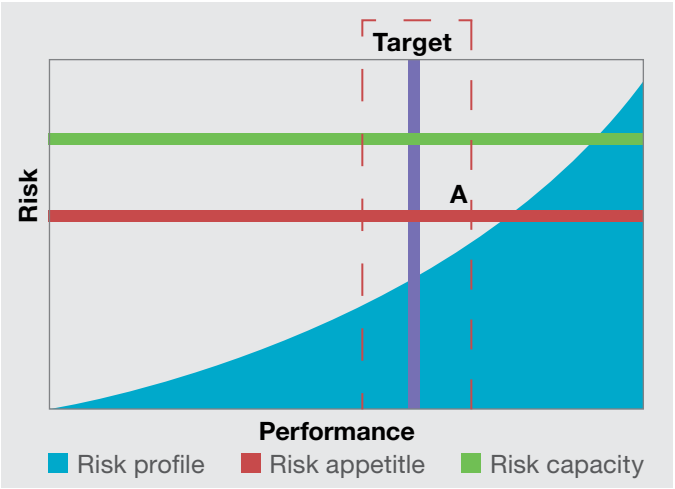
79. On any depiction of risk profile, organizations may also plot risk capacity (as in Figure 4.2), which is the maximum amount of risk an entity is able to absorb in the pursuit of strategy and business objectives. Risk capacity must be considered when setting risk appetite, as generally an organization strives to hold risk appetite within its capacity. It is not typical for an organization to set risk appetite above its risk capacity, but in rare situations an organization may accept the threat of insolvency and failure to exist on a strategic direction, understanding that success can create considerable value. (Additional discussion on risk profiles is presented in Appendix C.)

Considering Acceptable Variation in Performance

80. Closely linked to risk appetite is acceptable variation in performance, which is sometimes referred to as "risk tolerance." Both terms refer to the boundaries of acceptable outcomes related to achieving a business objective (both the boundary of exceeding the target and the boundary of trailing the target). Figure 4.3 illustrates acceptable variation in performance.

81. Having an understanding of acceptable variation in performance enables management to enhance value to the entity. For instance, the right boundary of acceptable variation should generally not exceed the point where the risk profile intersects risk appetite. But where the right boundary is below risk appetite, management may be able to shift its targets and still be within its overall risk appetite. The optimal point is where the right boundary of acceptable variation in performance intersects with risk appetite ("A" in Figure 4.3).

Figure 4.3: Risk Profile Showing Acceptable Variation in Performance



Risk Profiles in Action

82. Using risk profiles help management to determine what amount of risk is acceptable and manageable in the pursuit of strategy and business objectives. Risk profiles may help management:

- Find the optimal level of performance given the organization's ability to manage risk (i.e., where the organization positions the target).
- Determine the acceptable variation in performance related to the target (i.e., where the organization establishes leading or trailing performance targets).
- Understand the level of performance in the context of the entity's risk appetite (i.e., where the organization is in relation to the risk appetite).
- Identify where the organization may choose to take on more risk to enhance performance.

83. While the risk profile figures shown here imply needing a specific level of precision, and perhaps data, to create, keep in mind that these depictions can also be developed using qualitative information. Doing so helps to enhance the conversations of risk, risk appetite, acceptable variation in performance, and the overall relationship to performance targets.

5. Components and Principles

Components and Principles of Enterprise Risk Management

84. The Framework (Chapters 6 through 10) consists of the five interrelated components of enterprise risk management. Figure 5.1 illustrates these components and their relationship with the entity's mission, vision, and core values, and how they affect the entity's performance. Enterprise risk management is not static but iterative, and it is integrated into strategy planning and day-to-day decision-making.

Figure 5.1: Enterprise Risk Management Components

85. The five components are:

- **Risk Governance and Culture:** Risk governance and culture together form a basis for all other components of enterprise risk management. *Risk governance* sets the entity's tone, reinforcing the importance of, and establishing oversight responsibilities for, enterprise risk management. *Culture* pertains to ethical values, desired behaviors, and understanding of risk in the entity. Culture is reflected in decision-making.
- **Risk, Strategy, and Objective-Setting:** Enterprise risk management is integrated into the entity's strategic plan through the process of setting strategy and business objectives. With an understanding of business context, the organization can gain insight into internal and external factors and their impact to risk. An organization sets its risk appetite in conjunction with strategy-setting. The business objectives allow strategy to be put into practice and shape the entity's day-to-day operations and priorities.
- **Risk in Execution:** An organization identifies and assesses risks that may affect an entity's ability to achieve its strategy and business objectives. It prioritizes risks according to their severity and considering the entity's risk appetite. The organization then selects risk responses and monitors performance for change. In this way, it develops a portfolio view of the amount of risk the entity has assumed in the pursuit of its strategy and business objectives.
- **Risk Information, Communication, and Reporting:** Communication is the continual, iterative process of obtaining information and sharing it throughout the entity. Management uses relevant and quality information from both internal and external sources to support enterprise risk management. The organization leverages information systems to capture, process, and manage data and information. By using information that applies to all components, the organization reports on risk, culture, and performance.
- **Monitoring Enterprise Risk Management Performance:** By monitoring enterprise risk management performance, an organization can consider how well the enterprise risk management components are functioning over time and in light of substantial changes.

86. Within these five components are a series of principles, as illustrated in Figure 5.2. The principles represent the fundamental concepts associated with each component. These principles are worded as things organizations would do as part of the entity's enterprise risk management practices. While these principles are universal and form part of any effective enterprise risk management initiative, management must bring judgment to bear in applying them. Each principle is covered in detail in the respective chapters on components.

Figure 5.2: Enterprise Risk Management Principles

Assessing Enterprise Risk Management

87. An organization should have a means to reliably provide to the entity's stakeholders a reasonable expectation that it is able to manage risk associated with the strategy and business objectives to an acceptable level. It does this by assessing the enterprise risk management practices that are in place. Such assessment is voluntary, unless required otherwise by legislation or regulation. The Framework (Chapters 6 through 10) does not require that an assessment of the overall effectiveness of enterprise risk management be completed, but it does provide criteria for conducting one and making reasoned conclusions.

88. During an assessment, the organization may consider whether:

    - The components and principles relating to enterprise risk management are present and functioning.
    - The components relating to enterprise risk management are operating together in an integrated manner.
    - Controls necessary to effect principles are present and functioning.[9]

89. Components, relevant principles, and controls to effect those principles that are *present* exist in the design and implementation of enterprise risk management to achieve strategy and business objectives. Components, relevant principles, and controls to effect those principles that are *functioning* continue to operate to achieve strategy and business objectives. "Operating together" refers to the interdependencies of components and how they function cohesively.

90. Different approaches are available for assessing enterprise risk management. When the assessment is performed for the purpose of communicating to external stakeholders, it may be conducted considering the principles set out in the Framework (Chapters 6 through 10).

91. During an assessment, management may also review the suitability of those capabilities and practices, keeping in mind the entity's complexity and the benefits[10] the organization seeks to attain through enterprise risk management. Factors that add to complexity may include, among other things, the entity's geography; industry; nature; extent and frequency of change within the entity; historical performance and variation in performance; reliance on technology; and the extent of regulatory oversight.

9 Additional discussion on controls to effect principles is set out in *Internal Control—Integrated Framework.*

10 Potential benefits relating to enterprise risk management are set out in Chapter 1: Introduction.

Framework

6. Risk Governance and Culture

Chapter Summary

92. Risk governance and culture together form a basis for all other components of enterprise risk management. Risk governance sets the entity's tone, reinforcing the importance of enterprise risk management, and establishing oversight responsibilities for it. Culture pertains to ethical values, desired behaviors, and understanding of risk in the organization. Culture is reflected in decision-making.

Principles Relating to Risk Governance and Culture

1. **Exercises Board Risk Oversight**—The board of directors provides oversight of the strategy and carries out risk governance responsibilities to support management in achieving strategy and business objectives.
2. **Establishes Governance and Operating Model**—The organization establishes governance and operating structures in the pursuit of strategy and business objectives.
3. **Defines Desired Organizational Behaviors**—The organization defines the desired behaviors that characterize the entity's core values and attitudes toward risk.
4. **Demonstrates Commitment to Integrity and Ethics**—The organization demonstrates a commitment to integrity and ethical values.
5. **Enforces Accountability**—The organization holds individuals at all levels accountable for enterprise risk management, and holds itself accountable for providing standards and guidance.
6. **Attracts, Develops, and Retains Talented Individuals**—The organization is committed to building human capital in alignment with the strategy and business objectives.

Introduction

93. An entity's board of directors[11] plays an important role in risk governance and significantly influences enterprise risk management. Where the board is independent from management and generally comprises members who are experienced, skilled, and highly talented, it can offer an appropriate degree of industry, business, and technical input while performing its oversight responsibilities. This input includes scrutinizing management's activities when necessary, presenting alternative views, challenging organizational biases, and acting in the face of wrongdoing. Most important, in fulfilling its role of providing risk oversight, the board challenges management without stepping into the role of management.

94. Another critical influence on enterprise risk management is culture. Whether the entity is a small family-owned private company, a large, complex multinational, a government agency, or a not-for-profit organization, its culture reflects the entity's ethics: the values, beliefs, attitudes, desired behaviors, and understanding of risk. Culture supports the achievement of the entity's mission and vision. An entity with a risk-aware culture stresses the importance of managing risk and encourages transparent and timely flow of risk information. It does this with no assignment of blame, but with an attitude of understanding, accountability, and continual improvement.

Principle 1: Exercises Board Risk Oversight

The board of directors provides oversight of the strategy and carries out risk governance responsibilities to support management in achieving strategy and business objectives.

Accountability and Responsibility

95. The board of directors has the primary responsibility for risk oversight in the entity, and in many countries it has a fiduciary responsibility to its stakeholders, including conducting reviews of enterprise risk management practices. Typically, the full board retains responsibility for risk oversight, leaving the day-to-day responsibilities of managing and overseeing risk to management or a dedicated committee, such as a risk committee. Regardless of the structure, it is common to document responsibilities in a charter that defines the board's accountability versus management's accountability.

Skills, Experience, and Business Knowledge

96. The board of directors is well positioned to offer appropriate expertise and to understand and govern risk to the entity through its collective skills, experience, and business knowledge. This includes, for instance, asking the appropriate questions to challenge management when necessary about strategy, business objectives, plans, and performance targets. It also includes interacting with external stakeholders and presenting alternative views and actions.

97. Risk oversight is possible only when the board understands the entity's strategy and industry, and stays informed on issues affecting the entity. As strategy and the business context changes, so does

11 This Framework uses the term "board of directors" or "board" to encompass the governing body, including board, supervisory board, board of trustees, general partners, or owner.

risk in the operating model and risks to the strategy and business objectives. Consequently, the required qualifications for board membership may change over time. Each board must determine for itself, and review periodically, if it has the appropriate skills, expertise, and composition to provide effective risk oversight. For example, cyber risk is a reality for most entities, so entities exposed to cyber risk need to have board members who either have expertise in information technology or access to the required expertise through independent advisors or external consultants.

Independence

98. The board overall must be independent to be effective. Independence allows directors to be objective and to evaluate the performance and well-being of the entity without any conflict of interest or undue influence of interested parties. The board demonstrates its independence through each board member displaying his or her individual objectivity (see Example 6.1).

Example 6.1: Factors that Impede Board Independence

99. A board member's independence may be impeded if he or she:

- Holds a substantial financial interest in the entity.
- Is currently or has recently been employed in an executive role by the entity.
- Has recently advised the board of directors in a material way.
- Has a material business relationship with the entity, such as being a supplier, customer, or outsourced service provider.
- Has an existing contractual relationship with the entity (other than a directorship relationship).
- Has donated a significant financial amount to an entity.
- Has business or personal relationships with key stakeholders within an entity.
- Sits as a board member of other entities that represent a potential conflict of interest.

100. An independent board serves as a check and balance on management, ensuring that the entity is being run in the best interests of its stakeholders rather than of a select number of board members or management.

Suitability of Enterprise Risk Management

101. It is important that the board understand the complexity of the entity and how enterprise risk management will help the entity, including what benefits it will derive. Suitability of enterprise risk management refers to its ability to manage risk to an acceptable amount. The board helps define those desired benefits by engaging in conversations with management to determine whether enterprise risk management is suitable for the entity's needs. The board also works with management to define the operating model, reporting lines, and capabilities to achieve those benefits.

102. For example, some organizations may see the benefit of enterprise risk management as "gaining an understanding of the risks to the strategy." In this case, management would focus enterprise risk management on practices to achieve the strategy and business objectives—perhaps ways to reduce surprises and losses, or to reduce performance variability. Other organizations may define the value of enterprise risk management as "gaining an understanding of the risk of the strategy not aligning." Still others may consider the value of enterprise risk management as "its ability to support the achievement of mission, vision, and core values and the implications of the chosen strategy on its risk profile." In this case, management would focus more on strategy-setting and aligning the business objectives with day-to-day execution.

Organizational Bias

103. Bias in decision-making has always existed and always will. It is not unusual to find within an entity evidence of "groupthink," dominant personalities, overreliance on numbers, disregard of contrary information, disproportionate weighting of recent events, and a tendency for risk avoidance or risk taking. So the question is not whether bias exists, but rather how bias within enterprise risk management can be managed. The board is expected to understand the potential organizational biases that exist and challenge management to overcome them.

Principle 2: Establishes Governance and Operating Model

The organization establishes governance and operating structures in the pursuit of strategy and business objectives.

Operating Model and Reporting Lines

104. The organization establishes an operating model and designs reporting lines to execute the strategy and business objectives. In designing reporting lines within the operating model, it is important for the organization to clearly define responsibilities. The organization may also enter into relationships with external third parties that can influence reporting lines (e.g., strategic business alliances or joint business ventures).
105. Different operating models may result in different perspectives of a risk profile, which may affect enterprise risk management practices. For example, assessing risk within a decentralized operating model may indicate few risks, while the view within a centralized model may indicate a concentration of risk—perhaps relating to certain customer types, foreign exchange, or tax exposure.
106. The organization considers these and other factors when deciding what operating model to adopt. These factors also influence the design of enterprise risk management practices within operating units and functions. For example, the board of directors determines which management roles have at least a dotted line to the board to allow for open communication of all important issues. Similarly, direct reporting and informational reporting lines are defined at all levels of the entity.
107. Factors for establishing and evaluating operating models may include the:
    - Entity's strategy and business objectives.
    - Nature, size, and geographic distribution of the entity's business.
    - Risks related to the entity's strategy and business objectives.
    - The assignment of authority, accountability, and responsibility to all levels of the entity.
    - Type of reporting lines (e.g., direct reporting/solid line versus secondary reporting) and communication channels.
    - Financial, tax, regulatory, and other reporting requirements.

Enterprise Risk Management Structures

108. Management plans, organizes, and executes the entity's strategy and business objectives in accordance with the entity's mission, vision, and core values. Consequently, management needs information on how risk associated with the strategy occurs across the entity. One method of gathering such information is to delegate the responsibility to a committee. Committee members are typically executives or senior leaders appointed or elected by management, and each contributes individual skills, knowledge, and experience. Collectively, the committee provides risk oversight.

109. Entities with complex structures may have several committees, each with different but overlapping management membership. This multi-committee structure is then aligned with the operating model and reporting lines, which allows management to make business decisions as needed, with a full understanding of the risks inherent in those decisions.

110. Regardless of the particular management committee structure established, it is common to clearly state the authority of the committee, the management members who are a part of the committee, the frequency of meetings, and the specific responsibilities and operating principles the committee focuses on. In small entities, enterprise risk management oversight may be less formal, with management being much more involved in day-to-day execution.

Authority and Responsibilities

111. In an entity that has a single board of directors, the board delegates to management the authority to design and implement practices that support the achievement of strategy and business objectives. In turn, management defines roles and responsibilities for the overall entity and its operating units. Management also defines roles, responsibilities, and accountabilities of individuals, teams, divisions, operating units, and functions aligned to strategy and business objectives.

112. In an entity with dual boards, a supervisory board focuses on longer-term decisions and strategies impacting the business. A management board is charged with overseeing day-to-day operations including the oversight and delegation of authority among senior management. Similar to a single board governance model, management defines roles and responsibilities for the overall entity and its operating units.

113. Key roles typically include the following:

    - Individuals in a management role who have the authority and responsibility to make decisions and oversee business practices to achieve strategy and business objectives. Within the management team, the chief risk officer[12] is often the individual responsible for providing expertise and coordinating risk considerations.
    - Other personnel who understand both the entity's standards of conduct and business objectives in relation to their area of responsibility and the related enterprise risk management practices at their respective levels of the entity.

114. Management delegates authority and responsibility to enable personnel to make decisions. Periodically, management may revisit its structures by reducing layers of management, delegating more authority and responsibility to lower levels, or partnering with other entities.

12 The person delegated authority for enterprise risk management; other names for this role may be "head of enterprise risk management," "head of risk," "director of enterprise risk management," or "director of risk."

115. Clearly defining authority is important, as it empowers people to act as needed in a given role but also puts limits on authority. Risk-based decisions are enhanced when management:

    - Delegates authority only to the extent required to achieve the entity's strategy and business objectives (e.g., the review and approval of new products involves the business and support functions, separate from the sales team).
    - Specifies transactions requiring review and approval (e.g., management may have the authority to approve acquisitions).
    - Considers new and emerging risks as part of decision-making (e.g., a new vendor is not taken on without exercising due diligence).

Enterprise Risk Management within the Evolving Entity

116. As an entity changes, the capabilities and value it seeks from enterprise risk management may also change. Enterprise risk management should be tailored to the capabilities of the entity, considering both what the organization is seeking to attain and the way it manages risk. It is natural for the operating model to change as the nature of the business and its strategy evolves. Management, therefore, regularly evaluates the operating model and associated reporting lines.

117. In today's world of evolving information technology, new operating models are emerging. It may be that standard operating models soon become "virtual" in nature, relying far less on physical locations and more on technological interconnections. Such a shift requires examining how risk will also shift in response: At what point in decision-making is risk considered? How does this affect the achievement of strategy and business objectives? Management must be prepared to address these questions under a new operating model and understand how changes due to innovation will influence enterprise risk management practices.

Principle 3: Defines Desired Organizational Behaviors

The organization defines the desired behaviors that characterize the entity's core values and attitudes toward risk.

Culture Characteristics and Desired Behaviors

118. An entity's culture is reflected in its core values and approach to enterprise risk management. Culture is evident in decisions made throughout the entity—decisions ranging from those made about developing and implementing strategy to those affecting day-to-day tasks.

119. An entity's culture influences how the organization applies this Framework: how it identifies risk, what types of risk it accepts, and how it manages risk. Establishing a culture that is embraced by all personnel—one in which people do the right thing at the right time—is critical to the organization being able to seize opportunities and minimize risk to achieve the strategy and business objectives. It is up to the board of directors and management to define desired behaviors of the entity as a whole and of individuals within it. The culture drives the desired behaviors in day-to-day decision-making in order to meet the expectations of internal and external stakeholders.

120. A well-developed culture does not imply a template approach to enterprise risk management. That is, managers of some operating units may be prepared to take more risk, while others may be more conservative. For example, an aggressive sales unit may focus its attention on making a sale without careful attention to regulatory compliance outside the desired risk appetite, while the personnel in the contracting unit may focus on full compliance well within the desired risk appetite. Working separately, these two units could adversely affect the entity, but by working together, they can respond appropriately within the defined risk appetite to achieve the strategy and business objectives.
121. Many factors shape entity culture. Internal factors include, among others, how entity employees interact with each other and their managers, the standards and rules, the physical layout of the workplace, and the reward system in place. External factors include regulatory requirements and expectations of customers, investors, and others.
122. All these factors influence where the entity falls on the culture spectrum, which ranges from risk averse to risk aggressive (see Figure 6.1). The closer an entity is to the risk aggressive end of the spectrum, the greater is its propensity for and acceptance of the types and amount of risk necessary to achieve strategy and business objectives (see also Example 6.2).

Figure 6.1: Culture Spectrum

Example 6.2: Culture Spectrum

123. A nuclear power plant will likely have a risk-averse culture in its day-to-day operations. Both management and external stakeholders expect decisions regarding new technologies and systems to be made carefully and with great attention to detail and safety in order to provide reasonable expectation of the plant's reliability. It is not desirable for nuclear power plants to invest heavily in innovative and unproven technologies critical to managing the operations.
124. In contrast, a hedge fund is likely a risk aggressive entity. Management and external investors will have high expectations of performance that require taking on potentially severe risks, while still falling within the defined risk appetite of the entity.

Embracing a Risk-Aware Culture

125. Management defines the characteristics needed to achieve the desired culture over time, with the board providing oversight and focus. An organization can embrace a risk-aware culture by:

- *Maintaining strong leadership*: The board and management places importance on creating the right risk awareness and tone throughout the entity. Culture and, therefore, risk awareness, cannot be changed from second-line functions alone; the organization's leadership must be the real driver of change.
- *Employing a participative management style*: Management encourages personnel to participate in decision-making and to discuss risks to the strategy and business objectives.
- *Enforcing accountability for all actions*: Management documents policies of accountability and adheres to them, demonstrating to personnel that lack of accountability is not tolerated and that practicing accountability is appropriately rewarded.
- *Embedding risk in decision-making*: Management addresses risk consistently when making key business decisions, which includes discussing and reviewing risk scenarios that can help everyone understand the interrelationship and impacts of risks before finalizing decisions.

- *Having open and honest discussions about risks facing the entity*: Management does not view risk as being negative, but as being critical to achieving the strategy and business objectives.
- *Encouraging risk awareness across the entity*: Management continually sends messages to personnel that managing risk is a part of their daily responsibilities, and that it is not only valued but also critical to the entity's success and survival.
- *Communicating openly and reporting about risk*: Management is transparent about risk across the entity.

126. In a risk-aware culture, personnel know what the entity stands for and the boundaries within which they can operate. They can openly discuss and debate which risks should be taken to achieve the entity's strategy and business objectives, with the result being employee and management behaviors that are aligned with the entity's risk appetite.

Principle 4: Demonstrates Commitment to Integrity and Ethics

The organization demonstrates a commitment to integrity and ethical values.

Setting Tone throughout the Organization

127. The tone of an organization is fundamental to enterprise risk management. Without a strong and supportive tone that is communicated from the top of the organization—in support of an ethical culture—risk awareness can be undermined, responses to risks may be inappropriate, information and communication channels may falter, and feedback from monitoring entity performance may not be heard or acted on.

128. Tone is defined by the operating style and personal conduct of both management and the board of directors. Their formal acknowledgment of the risks send a message to the organization. When management and the board of directors behave ethically and responsibly, and demonstrate a commitment to addressing misconduct, they communicate to everyone that the organization strongly supports integrity. But where there are personal indiscretions, lack of receptiveness to bad news, or unfairly balanced compensation programs, the message sent may be one of indifference, which could negatively affect the culture and provoke inappropriate conduct. Personnel are likely to develop the same attitudes about what is acceptable and unacceptable—and about risks and risk responses—as those held by management.

129. Having a consistent tone helps an organization establish a common understanding of the core values, business drivers, and desired behavior of personnel and business partners. Consistency helps pull the organization together in the pursuit of the entity's strategy and business objectives. But it is not always easy to maintain a consistent tone. For instance, different markets and challenges may call for different approaches to motivation, evaluation, and customer service. From time to time, these factors may put pressure on different levels of the entity, resulting in a change in tone. (In larger entities, this view of tone is sometimes referred to as "tone in the middle.") However, the more the tone can remain consistent throughout the entity, the more consistent will be the performance of enterprise risk management responsibilities in the pursuit of the entity's strategy and business objectives.

Establishing and Evaluating Standards of Conduct

130. Standards of conduct guide the organization in its pursuit of strategy and business objectives by:
    - Establishing what is acceptable and unacceptable.
    - Providing guidance for navigating what lies between acceptable and unacceptable.
    - Reflecting laws, regulations, standards, and other expectations that the entity's stakeholders may have, such as corporate social responsibility.
131. Ethical expectations and norms vary across geographies and entities. Therefore, management and the board of directors establish the appropriate standards and mechanisms for adhering to them, which includes addressing the potential for non-compliance. These expectations are then transcribed onto an organizational statement—a code of conduct. The purpose of a code of conduct is to communicate the organization's expectations of ethics and desired behaviors, including behaviors relating to enterprise risk management and decision-making.
132. The organization demonstrates its commitment to applying the code of conduct when faced with difficult decisions. For example, when having to make a challenging decision, the organization might ask the following questions:
    - Does it infringe on the entity's standards of conduct?
    - Is it legal?
    - Would we want our shareholders, customers, regulators, external parties, or other stakeholders to know about it?
    - Would it reflect negatively on the individual or the entity?
133. The entity's standards of integrity and ethical values should be core messages in all forms of communications with personnel: for example, policies, training, and employment or service contracts. Some organizations require personnel to formally acknowledge receipt of and compliance with standards.
134. Training programs are also important to establishing standards of conduct. Those entities that are regularly recognized as being "a best place to work" and have high employee retention rates typically provide training on corporate ethical values. Generally, training sessions are conducted quarterly or biannually depending on the number of new personnel hired. During such training, personnel learn how the ethical climate has developed in the entity and the importance of speaking up and raising concerns. In addition, personnel are provided with examples of how integrity and ethical values have helped to identify issues and solve problems in the past.
135. With standards of conduct in place, an organization can evaluate the adherence to integrity and ethics. For example, an organization may establish a policy with measurable indicators to monitor and manage its ability to drive an ethical entity in line with its core values.

Responding to Deviations to Standards

136. When standards of conduct are not adhered to, it is generally for one of the following reasons:
    - Tone at the top does not effectively convey expectations.
    - The board does not provide oversight of management's adherence to standards.
    - Middle management and functional managers are not aligned with the entity's mission, vision, core values, strategy, and risk responses.
    - Risk is an afterthought to strategy-setting and business planning.
    - Performance targets create incentives or pressures to compromise ethical behavior.

- There is no clear escalation policy on important risk and compliance matters.
- The process for investigating and resolving excessive risk taking is inadequate.
- Intentional or deliberate non-compliance by management or personnel exists.

137. The organization sends a clear message of what is acceptable and unacceptable behavior whenever deviations become known. Deviations from standards of conduct must be addressed in a timely and consistent manner (see Example 6.3).

Example 6.3: When Deviations to Standards of Conduct Occur

138. For a global pharmaceutical company, research and development (R&D) is often one of the biggest costs, as products may take 10 to 20 years to develop and bring to market, with significant financial investment. During the research phase, it is common for many side effects of a product to be identified. But if R&D did not disclose all potential side effects to management so that they could make an informed decision on moving beyond drug trials to production, and the drug was launched, there could be severe impacts to the entity. Moreover, R&D's failure to disclose would likely be a clear violation of the desired conduct of the company.

139. The response to a deviation will depend on its magnitude, which is determined by management considering any relevant laws and standards of conduct. The response may range from an employee being issued a warning and provided with coaching, being put on probation, or even being terminated. In all cases, the entity's standards of conduct must remain consistent. Consistency ensures that the entity's culture is not undermined.

Aligning Culture, Ethics, and Individual Behavior

140. If establishing a culture in which management and personnel "do the right thing at the right time" is fundamental to enterprise risk management, then why do things sometimes go wrong? Even in those entities that solidly demonstrate integrity and ethics, scandals and crises do sometimes occur—damaging reputations and ultimately leaving an organization unable to achieve its strategy and business objectives.

141. Wrongdoing occurs for three reasons: good people make mistakes (out of confusion or ignorance), good people have a moment of weakness of will, and bad people choose to do harm. Knowing that any one of these three things can take place, an organization must align ethics and culture to help people avoid mistakes and maintain strong will, and to identify potential wrongdoers, individuals, or groups. This requires appropriately assessing and prioritizing risks and developing detailed risk responses.

142. Aligning individual behavior with culture is critical. The most powerful influence comes from management who creates and sustains the organizational agenda. Explicitly, the organization develops policies, rules, and standards of conduct. Implicitly, the organization "walks the talk" of core values and standards of conduct. The key is management enforcing what it says is of value, recognizing that it is the implicit and subtle processes that most effectively establish culture. People respond better to behavioral reinforcement than to written rules and policies.

143. Culture and ethics are integral to the entity's ability to achieve its mission and vision, but while culture is a powerful force, it is not a determining one; individual decision-making, and thus individual accountability, is fundamental to ethics and enterprise risk management.

Keeping Communication Open and Free from Retribution

144. It is management's responsibility to cultivate open communication and transparency about risk and the risk-taking expectations. Management demonstrates that risk is not a discussion to be left for the boardroom. It does that by sending clear and consistent messages to employees that managing risk is a part of everyone's daily responsibilities, and that it is not only valued but also critical to the entity's success and survival. Open communication and risk transparency enables management and personnel to work together continually to share risk information throughout the entity. In addition, management provides the board of directors with an appropriate amount of risk information to gauge whether current enterprise risk management practices are appropriate. The board of directors can provide risk oversight only if it is given timely and complete information, and when the lines of communication are open to discuss risk issues with management in the first and second lines of accountability.
145. The entity that demonstrates open communication and transparency provides a variety of channels for both management and personnel to report concerns about potentially inappropriate or excessive risk taking, business conduct, or behavior without fear of retaliation or intimidation. The entity also prohibits any form of inappropriate retaliation against any individual who participates in good faith in any investigation of behavior that is not in line with the standards of conduct and risk appetite. Personnel who engage in inappropriate or unlawful retaliation or intimidation are subject to disciplinary action.

Principle 5: Enforces Accountability

The organization holds individuals at all levels accountable for enterprise risk management, and holds itself accountable for providing standards and guidance.

Enforcing Accountability

146. The board of directors ultimately holds the chief executive officer[13] accountable for managing the risk faced by the entity by establishing enterprise risk management practices and capabilities to support the achievement of the entity's strategy and business objectives. The chief executive officer, chief risk officer, and other members of management, together, are responsible for all aspects of accountability—from initial design to periodic assessment of the culture and enterprise risk management capabilities. Accountability for enterprise risk management is demonstrated in each structure used by the entity.
147. Management provides guidance to personnel so they understand the risks. Management also demonstrates leadership by communicating the expectations of conduct for all aspects of enterprise risk management. Such leadership from the top helps to establish and enforce accountability, morale, and a common purpose.

13 This Framework refers to chief executive officer. Other senior leadership positions such as chief executive, president, managing director, or deputy may also apply to this role.

148. Accountability is evident in the following ways:

- Management and the board of directors being clear on the expectations (e.g., a code of conduct is developed and enforced).
- Management ensuring that information on risk flows throughout the entity (e.g., communicating how decisions are made and how risk is considered as part of decisions).
- Employees being committed to collective business objectives (e.g., aligning individual targets and performance with the entity's business objectives).
- Management responding to deviations from standards and behaviors (e.g., terminating personnel or taking other corrective actions for failing to adhere to organizational standards; initiating performance evaluations).

Holding Itself Accountable

149. In some governance structures, performance targets cascade from the board of directors to the chief executive officer, management, and other personnel, and performance is evaluated at each of these levels. The board of directors evaluates the performance of the chief executive officer, who in turn evaluates the management team, and so on. At each level, adherence to standards of conduct and desired levels of competence is evaluated, and rewards are allocated or disciplinary action is applied as appropriate. The board may also conduct a self-evaluation to assess its own strengths and identify opportunities to improve enterprise risk management.

150. In other governance structures, such as a two-tier board, the supervisory board evaluates the performance of the executive board as a whole and of its individual members; the executive board evaluates the management team that reports directly to the executive board.

Rewarding Performance

151. Performance is greatly influenced by the extent to which individuals are held accountable and how they are rewarded. It is up to management and the board of directors to establish incentives and other rewards appropriate for all levels of the entity, considering the achievement of both short-term and longer-term business objectives. Establishing such incentives and rewards requires appropriately assessing and prioritizing risks and developing detailed risk responses. Conversely, under a program of incentives, those individuals who do not adhere to the entity's standards of conduct are sanctioned and not promoted or otherwise rewarded.

152. Salary increases and bonuses are common incentives, but non-monetary rewards such as being given greater responsibility, visibility, and recognition are also effective. Management should consistently apply and regularly review the organization's measurement and reward structures in conjunction with its standards of conduct and desired behavior. In doing so, the performance of individuals and teams are reviewed in relation to defined measures, which include business performance factors as well as demonstrated competence (see Example 6.4).

Example 6.4: Performance, Incentives, and Rewards

153. A family-owned furniture manufacturer is trying to win customer loyalty with its high-quality furniture. It engages its workforce to reduce production defect rates, and it aligns its performance measures, incentives, and rewards with both the operating unit's production goals and the expectation to comply with all safety and quality standards, workplace safety laws, customer loyalty programs, and accurate product recall reporting. In this way, the business objectives of achieving customer loyalty and selling high-quality furniture, understanding the risks through defects, and considering safety are all aligned with business performance, incentives, and rewards.

Addressing Pressure

154. Pressure in an organization comes from many sources. The targets that management establishes for achieving strategy and business objectives by their nature create pressure. Pressure also may occur during the regular cycles of specific tasks (e.g., negotiating a sales contract), and it may sometimes be self-imposed. Unexpected external factors, such as a sudden dip in the economy, can also add pressure.

155. Pressure can either motivate individuals to meet expectations, or cause them to fear the consequences of not achieving strategy and business objectives. In the latter case, there is risk that individuals may circumvent processes or engage in fraudulent activity. Organizations can positively influence pressure by rebalancing workloads or increasing resource levels, as appropriate, to reduce this risk and continue to communicate the importance of ethical behavior.

156. Excessive pressure is most commonly associated with:

- Unrealistic performance targets, particularly for short-term results.
- Conflicting business objectives of different stakeholders.
- Imbalance between rewards for short-term financial performance and those for long-term focused stakeholders, such as corporate sustainability targets (see Example 6.5).

Example 6.5: The Price of Pressure

157. The pressures to demonstrate the profitability of investment strategies can cause traders to take off-strategy risks with unapproved products to cover incurred losses. Similarly, the pressure to rush a product to market and generate revenues quickly may cause personnel within a pharmaceutical company to take shortcuts on product development or safety testing, which could prove harmful to consumers or lead to poor acceptance or impaired reputation.

158. Possible negative reaction to pressure should be accounted for when considering compensation and incentives. For example, investment managers take risks on behalf of their client portfolios, and the performance of those investments may significantly affect the entity's remuneration. A fee model based on fund performance may result in very different behavior within the entity compared with a fund value model. Aligning an individual's compensation to the organizational structure can help achieve strategy and business objectives. Conversely, incentive structures that fail to adequately consider the risks associated with the organizational structure can create inappropriate behavior.

159. Pressure is also created by change: change in strategy, in operating model, in acquisition or divestiture activity, and in the business context, which is often external to the organization, such as market competitor actions. Management and the board must be prepared to set and adjust, as appropriate, the pressure when assigning responsibilities, designing performance measures, and evaluating performance. It is management's responsibility to guide those to whom they have delegated authority to make appropriate decisions in the course of doing business.

Principle 6: Attracts, Develops, and Retains Talented Individuals

The organization is committed to building human capital in alignment with the strategy and business objectives.

Establishing and Evaluating Competence

160. Management, with board oversight, defines the human capital needed to carry out strategy and business objectives. Understanding the needed competencies helps in establishing how various business processes should be carried out and what skills should be applied. This begins with the board of directors relative to the chief executive officer, and the chief executive officer relative to each of the management and personnel of divisions, operating units, and functions in the entity. That is, the board of directors evaluates the competence of the chief executive officer and, in turn, management evaluates competence across the entity and addresses any shortcomings or excesses as necessary.

161. The human resources function helps promote competence by developing job descriptions and roles and responsibilities, facilitating training, and evaluating individual performance for managing risk. Management considers the following factors when developing competence requirements:

- Knowledge, skills, and experience with enterprise risk management.
- Nature and degree of judgment and limitations of authority to be applied to a specific position.
- The costs and benefits of different skill levels and experience.

Attracting, Developing, and Retaining Individuals

162. The ongoing commitment to competence is supported by and embedded in the human resource management processes. Management at different levels establishes the structure and process to:

- *Attract*: Seek out the necessary number of candidates who fit the entity's risk-aware culture, desired behaviors, operating style, and organizational needs, and who have the competence for the proposed roles.
- *Train*: Enable individuals to develop and maintain enterprise risk management competencies appropriate for assigned roles and responsibilities, reinforce standards of conduct and desired levels of competence, tailor training to specific needs, and consider a mix of delivery techniques, including classroom instruction, self-study, and on-the-job training.
- *Mentor*: Provide guidance on the individual's performance regarding standards of conduct and competence, align the individual's skills and expertise with the entity's strategy and business objectives, and help the individual to adapt to an evolving internal environment and external environment.
- *Evaluate*: Measure the performance of individuals in relation to achieving business objectives and demonstrating enterprise risk management competence against service-level agreements or other agreed-upon standards.
- *Retain*: Provide incentives to motivate an individual, and reinforce the desired level of performance and conduct. This includes offering training and credentialing as appropriate.

163. Throughout this process, any behavior not consistent with standards of conduct, policies, performance expectations, and enterprise risk management responsibilities is identified, assessed, and corrected in a timely manner.

164. In addition, organizations must continually identify and evaluate those roles that are essential to achieving strategy and business objectives. The decision of whether a role is essential is made by assessing the consequences of having that role temporarily or permanently unfilled. The question needs to be asked: How will strategy and business objectives be achieved if the position of, for example, the chief executive officer is left unfilled?

Preparing for Succession

165. To prepare for succession, the board of directors and management must develop contingency plans for assigning responsibilities important to enterprise risk management. In particular, succession plans for key executives need to be defined, and succession candidates should be trained, coached, and mentored for assuming the role. Typically, larger entities identify more than one person who could fill a critical role.

7. Risk, Strategy, and Objective-Setting

Chapter Summary

166. Enterprise risk management is integrated into the entity's strategic plan through the process of setting strategy and business objectives. Business context influences risks that impact the entity. Risk appetite is established and aligned with strategy. Business objectives allow strategy to be put into practice and shape the entity's day-to-day operations and priorities.

Principles Relating to Risk, Strategy, and Objective-Setting

7. **Considers Risk and Business Context**—The organization considers potential effects of business context on risk profile.
8. **Defines Risk Appetite**—The organization defines risk appetite in the context of creating, preserving, and realizing value.
9. **Evaluates Alternative Strategies**—The organization evaluates alternative strategies and impact on risk profile.
10. **Considers Risk while Establishing Business Objectives**—The organization considers risk while establishing the business objectives at various levels that align and support strategy.
11. **Defines Acceptable Variation in Performance**—The organization defines acceptable variation in performance relating to strategy and business objectives.

Introduction

167. Every entity has a strategy for bringing its mission and vision to fruition, and to drive value. It can be a challenge to assess whether strategies and business objectives will align with mission, vision, and core values, but it is a challenge that must be taken on. By integrating enterprise risk management with strategy-setting, an organization gains insight into the risk profile associated with strategy and its execution. Doing so guides the organization and helps to sharpen the strategy and its execution.

Principle 7: Adapts to Business Context

The organization considers potential effects of business context on risk profile.

Understanding Business Context

168. An organization considers business context when developing strategy to support its mission, vision, and core values. "Business context" refers to the trends, relationships, and other factors that influence, clarify, or drive change to an organization's current and future strategy and business objectives. Business context may be:

- Dynamic, where new risks can emerge at any time causing disruption and changing the status quo (e.g., a new competitor causes product sales to decrease or even make the product obsolete).
- Complex, with many interconnections and interdependencies (e.g., an entity has many operating units around the world, each with its own unique political regimes, regulatory policies, and taxation laws).
- Unpredictable, as change may happen quickly and in unanticipated ways (e.g., currency fluctuations and political forces).

Considering External Environment and Stakeholders

169. The external environment is part of the business context. It is anything outside the entity that can influence the entity's ability to achieve its strategy and business objectives. External stakeholders are, in turn, part of the external environment.

170. An example of an external stakeholder is a regulatory body that grants an entity a license to operate, but also has the authority to fine the entity or force it to shut down temporarily or permanently. Another example is an investor who provides the entity with capital, but who can decide to take that investment elsewhere if it does not agree with the entity's strategic direction or its level of performance. An organization that identifies its external environment and stakeholders and the extent of their influence on the business will be in a better position to anticipate and adapt to change.

171. External stakeholders are not directly engaged in the entity's operations, but they:

- Are affected by the entity (customers, suppliers, competitors, etc.).
- Directly influence the entity's business environment (government, regulators, etc.).
- Influence the entity's reputation, brand, and trust (communities, interest groups, etc.).

172. Like external stakeholders, the external environment can influence an entity's ability to achieve its strategy and business objectives. The external environment comprises several factors that can be categorized by the acronym PESTLE:[14] political, economic, social, technological, legal, and environmental (Figure 7.1). Example 7.1 illustrates this concept.

Figure 7.1: External Environment Categories and Characteristics[15]

Categories	Characteristics of External Environment
Political	The nature and extent of government intervention and influence, including tax policies, labor laws, environmental laws, trade restrictions, tariffs, and political stability
Economic	Interest rates, inflation, foreign exchange rates, availability of credit, etc.
Social	Customer needs or expectations; population demographics, such as age distribution, educational levels, distribution of wealth
Technological	R&D activity, automation, and technology incentives; rate of technological changes or disruption
Legal	Laws (e.g., employment, consumer, health and safety), regulations, and industry standards
Environmental	Natural or human-caused catastrophes, ongoing climate change, changes in energy consumption regulations, attitudes toward the environment

Example 7.1: External Environment Influences

173. A global technology company is seeking to increase revenue by launching an established product in developing countries, while another technology company is developing a product for a new consumer base in its home country. As each company evaluates alternative strategies, they consider different external environment categories. The first company is influenced by political, legal, and economic factors as it navigates country-specific laws, government regulations, and capital considerations. In contrast, the second company focuses on social and technological factors as it seeks to understand the new customer needs. Even though both companies are in the same industry, they have different external environments that influence their specific risk profiles and, ultimately, their chosen strategy.

Considering Internal Environment[16] and Stakeholders

174. An entity's internal environment is anything inside the entity that can affect its ability to achieve its strategy and business objectives (Figure 7.2). Internal stakeholders are those people working within the entity who directly influence the organization (board directors, management, and other personnel). As entities vary greatly in size and structure, internal stakeholders may affect the organization differently as a whole than at the level of division, operating unit, or function (see Example 7.2).

14 PESTLE (also known as PEST, PESTEL, STEP, or STEEPLE) analysis was developed to analyze external environmental factors.

15 External environment categories may also be considered as potential risk categories when identifying and assessing risks.

16 Internal environment is explored in greater detail in the Risk Governance and Culture Component (Chapter 6).

Figure 7.2: Internal Environment Categories and Characteristics

Categories	Characteristics of Internal Environment
Capital	Assets, including cash, equipment, property, patents
People	Knowledge, skills, attitudes, relationships, core values, and culture
Process	Activities, tasks, policies, or procedures; changes in management, operational, and supporting processes
Technology	New, amended, or adopted technology

Example 7.2: External and Internal Environment Influences

175. An entity whose mission, vision, and core values support community-based labor in an economically challenged region considers how political, economic, social, and environmental factors may influence its ability to hire and maintain a skilled workforce. It considers the people and capabilities that are needed to support its mission, vision, and adhere to its core values. The organization is mindful of its ability to secure skilled labor when considering the risk profile associated with various strategies. Understanding these external and internal influences provides valuable insight when selecting a strategy.

How Business Context Affects Risk Profile

176. The effect that business context has on an entity's risk profile may be viewed in three stages: past, present, and future performance. Looking back at past performance can provide an organization with valuable information to use in shaping its risk profiles. Looking at current performance can show an organization how current trends, relationships, and other factors are affecting the risk profile. And by thinking what these factors will look like in the future, the organization can consider how its risk profile will evolve in relation to where it is heading or wants to head. Example 7.3 illustrates how an organization can consider business context with the components of enterprise risk management.

Example 7.3: Considering Business Context in Each of the Framework Components

- **Risk Governance and Culture:** Management of a retail company considers business context as it develops an understanding of interactions with its internal and external stakeholders. In doing so it considers broad megatrends shaping the industry.
- **Risk, Strategy, and Objective-Setting:** The company integrates its understanding of business context, for instance, megatrends, into the strategic planning cycle for long-term value and success.
- **Risk in Execution:** The company incorporates its understanding of business context into its risk identification, assessment, and response practices, potentially impacting risk today and in the future.
- **Risk Information, Communication, and Reporting:** The company considers how changes in business context may affect the way the organization captures, communicates, and reports on risk information.
- **Monitoring Enterprise Risk Management Performance:** The company considers how changes affecting business context may also affect the entity's culture and enterprise risk management practices, including opportunities to enhance current practices.

Principle 8: Defines Risk Appetite

The organization defines risk appetite in the context of creating, preserving, and realizing value.

Determining Risk Appetite

177. Risk appetite guides an organization in determining the types and amount of risk it is willing to accept. There is no standard or "right" risk appetite that applies to all entities. Management and the board of directors choose a risk appetite with full understanding of the trade-offs involved. Risk appetite may encompass a single depiction of the acceptable types and amount of risk or several depictions that align and collectively support the mission and vision of the entity.

178. A variety of approaches are available to determine risk appetite, including facilitating discussions, reviewing past and current performance targets, and modeling. It is up to management to communicate the agreed-upon risk appetite at various levels of detail throughout the entity. With the approval of the board, management also revisits and reinforces risk appetite over time in light of new and emerging considerations. Also, while risk appetite is extremely important in the consideration of strategy and when setting business objectives and performance targets, once an entity considers risk in execution, the focus shifts to managing risks within acceptable variation.

179. For some entities, using general terms such as "low appetite" or "high appetite" is sufficient. Others may view such statements as too vague to effectively communicate and implement, and therefore they may look for more quantitative measures. Often, as organizations become more experienced in enterprise risk management, their description of risk appetite becomes more precise. Some will develop a series of cascading expressions of risk appetite referencing "targets," "ranges," "floors," or "ceilings" (see Example 7.4). Others will use specific quantitative terms as a way of increasing precision.

Example 7.4: Sample Risk Appetite Expressions

- *Target:* A credit union with a lower risk appetite for loan losses cascades this message into the business by setting a loan loss target of 0.25% of the overall loan portfolio.
- *Range:* A medical supply company operates within a low overall risk range. Its lowest risk appetite relates to safety and compliance objectives, including employee health and safety, with a marginally higher risk appetite for its strategic, reporting, and operations objectives. This means reducing to a reasonably practicable amount the risks originating from various medical systems, products, equipment, and the work environment, and meeting legal obligations will take priority over other business objectives.
- *Ceiling:* A university accepts a moderate risk appetite as it seeks to expand the scope of its offerings where financially prudent and will explore opportunities to attract new students. The university will favor new programs where it has or can readily attain the requisite capabilities to deliver them. However, the university will not accept programs that present severe risk to the university mission and vision, forming a ceiling on acceptable decisions.
- *Floor:* A technology company has aggressive goals for growth in its sector, and recognizes that such growth requires significant capital investment. While it does not accept investing capital unwisely, management is of the view that, as a minimum, 25% (i.e., the floor) of the operating budget should be allocated to the pursuit of technology innovation.

180. An organization may consider any number of parameters to help frame its risk appetite and provide greater precision: For example, the organization may consider:

- Strategic parameters, such as new products to pursue or avoid, the investment for capital expenditures, and merger and acquisition activity.
- Financial parameters, such as the maximum acceptable variation in financial performance, return on assets or risk-adjusted return on capital, target debt rating, and target debt/equity ratio.
- Operating parameters, such as environmental requirements, safety targets, quality targets, and customer concentrations.

181. Management may also consider the entity's risk profile, risk capacity, risk capability and maturity, among other things, when determining risk appetite.

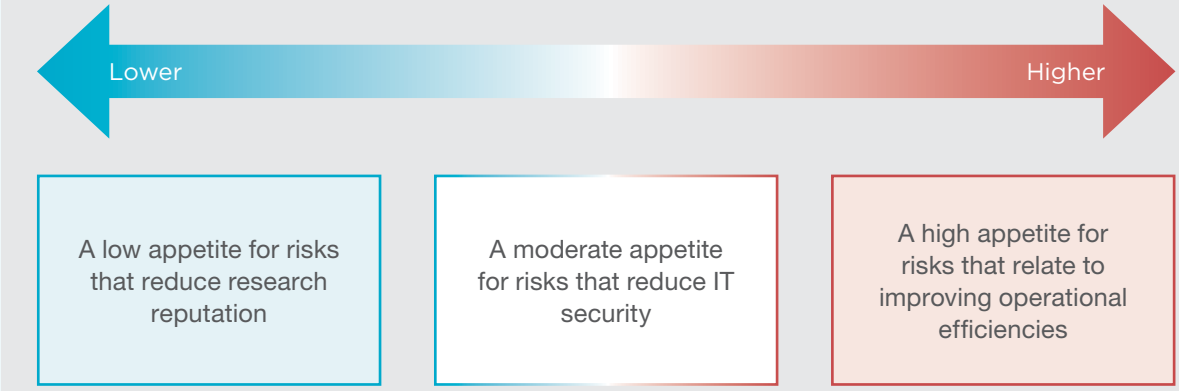
- *Risk profile* provides information on the entity's current amount of risk and how risk is distributed across the entity, as well as on the different categories of risk for the entity. New organizations will not have an existing risk profile to draw from, but they may be able to get valuable information from their industry and competitors.
- *Risk capacity*, which was introduced in Chapter 3, is the maximum amount of risk the entity can absorb. If risk appetite is very high, but its risk capacity is not large enough to withstand the potential impact of the related risks, the entity could fail. On the other hand, if the entity's risk capacity significantly exceeds its risk appetite, the organization may lose opportunities to add value for its stakeholders.
- *Enterprise risk management capability and maturity* provide information on how well enterprise risk management is functioning. A mature organization is often able to define enterprise risk management capabilities that provide better insight into its existing risk appetite and factors influencing risk capacity. A less mature organization with undefined enterprise risk management capabilities may not have the same understanding, which can result in a broader risk appetite statement or one that will need to be redefined sooner. Enterprise risk management capability and maturity also influence how the organization adheres to and operates within its risk appetite.

Articulating Risk Appetite

182. Some organizations articulate risk appetite as a single point; others as a continuum (see Example 7.5).

Example 7.5: Risk Appetite Continuum

183. A university has set its business objectives focusing on its role as a preeminent teaching and research university that attracts outstanding students and as a desired place of work for top faculty. The university's risk appetite statements acknowledge that risk is present in almost every activity. The critical question in establishing the risk appetite is how willing the university is to accept risk related to each area. To answer that question, management uses a continuum to express risk appetite for the university's major business objectives (teaching, research, service, student safety, and operational efficiency). They place various risks along the continuum as a basis for discussion at the highest levels.



184. An organization may articulate detailed risk appetite statements in the context of:

- Strategy and business objectives that align with the mission, vision, and core values.
- Business objective[17] categories.
- Performance targets of the entity.

185. Risk appetite is communicated by management, endorsed by the board, and disseminated throughout the entity. Disseminating risk appetite is important, as the goal is for all decision-makers to understand the risk appetite they must operate within and for all operations to be consistent with the risk appetite, especially those who execute tasks to achieve business objectives (e.g., local sales forces, country managers, operating units).

17 Establishing business objectives is discussed in Principle 10. They are included here to better illustrate how risk appetite cascades from strategy through business objectives.

186. Example 7.6 illustrates how one organization cascades risk appetite through statements aligned with high-level business objectives that, in turn, align with the overall entity strategy.

Example 7.6: Cascading Risk Appetite

Mission: To provide healthy, great-tasting premium organic foods made from locally sourced ingredients.	**Vision**: To be the largest producer of sustainable sourced organic products in the markets we serve.	**Core Values**: We work to achieve a healthy environment that is sustainable. We will use ingredients grown only in natural composts, non-altered crops, and soil rich in organic life.

Strategy: To build brand loyalty by producing food that is delicious and exciting, that people want to eat because it tastes good, not because it is good for them.	**Risk Appetite**: Brand is essential to us. We will strive to be innovative to develop products that meet customers' preferences. We will not put cost above our core values, product quality, or ingredient choice. Nor will we put growth above sustainable operations.
Business Objective: To continue to develop new, innovative products that interest and excite consumers.	**Risk Appetite**: We will continue to strive to be innovative and find new tastes. **Risk Appetite**: We will not compromise our brand by using products that are not certified organic. We accept that this may increase our cost.
Business Objective: To expand our retail presence in the higher-end health food sector.	**Risk Appetite**: We value our brand as a premium product and will focus only on those retailers that share our core values. We understand that this may affect our sales channel.

Applying Risk Appetite

187. Risk appetite guides how an organization allocates resources, both through the entire entity and in individual operating units. The goal is to align resource allocation with the entity's mission, vision, and core values. Therefore, when management allocates resources across operating units, it considers the entity's risk appetite and individual operating units' plans for creating value. Management also aligns people, processes, and infrastructure to successfully implement strategy while remaining within its risk appetite.

188. Risk appetite is incorporated into decisions on how the organization operates, and management, with board oversight, continually monitors risk appetite at all levels and accommodates change when needed. In this way, management creates a culture that emphasizes the importance of risk appetite and holds those responsible for implementing enterprise risk management within the risk appetite parameters.

Principle 9: Evaluates Alternative Strategies

The organization evaluates alternative strategies and impact on risk profile.

189. An organization must evaluate alternative strategies as part of its strategy-setting process and assess the risk and opportunities of each option. This evaluation is often referred to as "due diligence." Alternative strategies are assessed in the context of the organization's resources and capabilities to create, preserve, and realize value. A part of enterprise risk management includes evaluating strategies from two different perspectives of risk: (1) the possibility that the strategy does not align with the mission, vision, and core values of the entity, and (2) the implications of the chosen strategy.

The Importance of Aligning Strategy

190. Strategy must support mission and vision, as well as its core values, and align with the entity's culture and risk appetite. If it does not, the entity may not achieve its mission and vision.

191. Further, a misaligned strategy increases risk to stakeholders because the value of the organization and its reputation may be affected. For example, a telecommunications company is considering a strategy of limiting the areas in which its products and services are available in order to improve its financial performance. But this strategy is at odds with its mission of being a provider of critical services and a leading corporate citizen in the local community. While the anticipated improvement in financial results is intended to appeal to shareholders and investors, it may be undermined by an adverse impact to its reputation with community groups and regulators that insist that services be maintained.

Understanding the Implications of Chosen Strategies

192. When evaluating alternative strategies, the organization seeks to identify and understand the potential risks of each strategy being considered. The identified risks collectively form a risk profile for each option; that is, different strategies yield different risk profiles. Management and the board use these risk profiles when deciding on the best strategy to adopt, given the entity's risk appetite.

193. Another consideration when evaluating alternative strategies is the supporting assumptions relating to business context, resources, and capabilities. Where assumptions are unproven, there is often a higher risk of disruption than there would be if the organization knew with greater certainty that there would not be disruptive events associated with a strategy. The level of confidence of management and the board associated with each assumption will impact the risk profile of each of the strategies. Further, a strategy typically has a higher risk profile when a significant number of assumptions are made.

194. Once a risk profile has been defined for the chosen strategy, management is better able to consider the types and amount of risk it will face in executing that strategy. Specifically, knowing the risk profile allows management to determine what resources will be required and allocated to support executing the strategy while remaining within the risk appetite. Resource requirements include infrastructure, technical expertise, and working capital.

195. The amount of effort expended and the level of precision required in evaluating alternative strategies will vary depending on how significant the decision is, the resources and capabilities available, and the number of strategies being evaluated. The more significant the decision, the more detailed the evaluation will be, perhaps using several approaches (see Example 7.7).

Example 7.7: Evaluating Strategies

196. An industrial chemical company in a highly regulated industry needs to evaluate a strategy for taking a product to a new geographic market. This particular strategy represents a significant outlay of capital resources. The market is highly regulated, and the new geographic area presents different cultural implications, so management's evaluation must be extensive. Management reviewed barriers to entry, potential market share, competitor analysis, revenue forecasts, geographic/cultural analysis, supply chain analysis, and regulatory investigation.

197. At the same time, the company is considering changing its distribution partner in its supply chain. The decision associated with this strategy is less significant because no additional capital outlay is expected, and the change does not introduce a new regulatory market, so management's evaluation is less rigorous. In this case, they perform a cost analysis, quality control analysis, and value chain analysis.

198. Popular approaches to evaluating alternative strategies are SWOT analysis,[18] modeling, valuation, revenue forecast, competitor analysis, and scenario analysis. The evaluation (or due diligence) is typically performed by management personnel who have an entity-wide view of risk and understand how strategy affects performance. That is, management understands at the entity level how a chosen strategy will support performance across different divisions, functions, and geographies.

199. When developing alternative strategies, management makes certain assumptions. These underlying assumptions can be sensitive to change, and that propensity to change can greatly affect the risk profile. Once a strategy has been chosen, and by understanding the propensity of assumptions to change, the organization is able to develop requisite oversight mechanisms relating to changing assumptions. Example 7.8 illustrates one organization's process of evaluating alternative strategies.

Example 7.8: Considering Alternative Strategies

200. A global logistics service provider would like to expand operations to meet global demand, and to do so it needs a new distribution hub. During strategic planning, several alternatives are assessed.

- Alternative 1 is opening a distribution hub offshore in a developing country. This is the least expensive of the locations being considered both in cost to build and labor to run, but would increase delivery time by an average of 30%. Locating in this developing country also introduces geopolitical and economic risks.
- Alternative 2 is opening a distribution hub located onshore in a mid-size city. This location is a bit more expensive to build than alternative 1, but the labor supply is strong. However, winters are severe in the area, which heightens the risk that weather-related events will disrupt transportation.
- Alternative 3 is an onshore location in a larger city. This location is the most expensive to build in and has the most competitive labor market, which may result in increased operating costs. However, the climate is temperate all year round.

- **Mission:** To provide the highest quality transportation services to customers with safety being the foremost consideration for operations while maintaining strong financial returns for shareholders.
- **Vision:** Enhance our brand to be the go-to transportation provider for the globe.

18 SWOT is an acronym for strengths, weaknesses, opportunities, and threats. A SWOT analysis is a structured planning method that evaluates those four elements.

Example 7.8 continued

201. The possibility of the strategy not aligning with the mission and vision, and the implications from the strategy on the risk profile, are summarized below.

	Possibility of strategy not aligning with mission and vision	Implications from the strategy on the risk profile
Alternative 1	• Political instability may present future safety issues	• Additional delivery time may affect customer satisfaction and erode value • Increased geopolitical and economic risk
Alternative 2	• Snowstorms may present safety issues for planes and trucks • Shareholder value may suffer during down times	• Delivery times may be delayed because of poor winter weather conditions, which could affect customer satisfaction
Alternative 3	• Increased cost may erode shareholder value	• Labor costs may be higher • Increased costs could create pricing variances and drive down volume

Aligning Strategy with Risk Appetite

202. An organization should expect that the strategy it selects can be executed within the entity's risk appetite; that is, strategy must align with risk appetite. If the risk associated with a specific strategy is inconsistent with the entity's risk appetite or risk capacity, the strategy needs to be revised, an alternative strategy selected, or the risk appetite revisited.

203. For instance, a beverage manufacturer had this strategy: "To grow business by expanding global manufacturing locations." However, when it became clear that some global locations presented risk that exceeded the manufacturer's risk appetite, the strategy was updated: "To grow business by expanding to global locations within established infrastructure requirements and governmental regulations."

Making Changes to Strategy

204. Typically, organizations hold periodic strategy-planning sessions to outline both short-term and long-term strategies.[19] A change in strategy is warranted if the organization determines that the current strategy fails to create, realize, or preserve value; or a change in business context causes the entity to get too near the maximum amount of risk it is willing to accept, or require resources and capabilities that are not available to the organization. Finally, developments in business context may result in the organization no longer having a reasonable expectation that it can achieve the strategy (see Example 7.9).

Example 7.9: Making Changes to Strategy

205. A global camera manufacturer used to sell film cameras, but as digital cameras became more popular, the company's value started to erode due to lower sales. In response, it has modified its strategy by adapting to a changing consumer need and new technology. It now develops digital cameras and mitigates the risk that its products may become obsolete. These changes to strategy are supported by changes to relevant business objectives and performance targets.

19 Smaller entities may not have formal strategy-setting sessions, and strategy planning may be more ad hoc.

Mitigating Bias

206. Bias always exists, but an organization should try to be unbiased—or to mitigate any bias—when it is evaluating alternative strategies. The first step is to identify any bias that may exist during the strategy-setting process. The next step is to mitigate bias that is identified. Bias may prevent an organization from selecting the best strategy to both support the entity's mission, vision, core values, and to reflect the entity's risk appetite.

Principle 10: Considers Risk while Establishing Business Objectives

The organization considers risk while establishing the business objectives at various levels that align and support strategy.

Establishing Business Objectives

207. The organization develops business objectives that are measurable or observable, attainable, and relevant. Business objectives provide the link to practices within the entity to support the achievement of the strategy. For example, business objectives may relate to:

- *Financial performance:* Maintain profitable operations for all businesses.
- *Customer aspirations:* Establish customer care centers in convenient locations for customers to access.
- *Operational excellence:* Negotiate competitive labor contracts to attract and retain employees.
- *Compliance obligations:* Comply with applicable health and safety laws on all work sites.
- *Efficiency gains:* Operate in an energy-efficient environment.
- *Innovation leadership:* Lead innovation in the market with frequent new product launches.

208. Business objectives may cascade throughout the entity (divisions, operating units, functions) or be applied selectively. Cascading objectives become more detailed as they are applied progressively from the top of the entity down. For example, financial performance objectives are cascaded from divisional targets to individual operating units. Alternatively, many business objectives will be specific to an operational dimension, geography, product, or service.

Aligning Business Objectives

209. Individual objectives are aligned with strategy regardless of how the objective is structured and where it is applied. The alignment of business objectives to strategy supports the entity in achieving its mission and vision.

210. Business objectives that do not align, or only partially align, to the strategy will not support the achievement of the mission and vision and may introduce unnecessary risk to the risk profile of the entity. That is, the organization may consume resources that would otherwise be more effectively deployed in executing other business objectives.

211. Business objectives should also align with the entity's risk appetite. If they do not, the organization may be accepting either too much or too little risk. Therefore, when an organization evaluates a proposed business objective, it must consider the potential risks that may occur and determine the impact to the risk profile. A business objective that results in the organization exceeding the risk appetite may be modified or, perhaps, discarded.

212. If an organization finds that it cannot establish business objectives that support the achievement of strategy while remaining within its risk appetite or capabilities, a review of either the strategy or the risk profile is required.

Understanding the Implications of Chosen Business Objectives

213. An organization has many options when deciding on business objectives. Consider, for example, an organization that is presented with an opportunity to upgrade its core operating systems and redesign its existing IT infrastructure. One option is to pursue a business objective of identifying a suitable vendor and entering into a third-party arrangement to develop a customized IT system. Another option is for the organization to build its own system internally by investing significantly in its IT capabilities and increasing the number of personnel. Both objectives align with the overall strategy, and therefore management must evaluate both and determine the appropriate course of action given the potential implications to the risk profile, resources, and capabilities of the entity.

214. As is the case with setting strategy, the organization needs to have a reasonable expectation that a business objective can be achieved given the risk appetite or resources available to the entity. The expectation is informed by the entity's capabilities and resources. Where that reasonable expectation does not exist, the organization must choose to either exceed risk appetite, procure more resources, or change the business objective. Depending on the significance of the business objective to the strategy, revising the strategy may also be warranted (see Example 7.10).

Example 7.10: Determining the Implications of a Chosen Business Objective

215. As part of its five-year strategy, an agricultural producer is looking to cultivate organic produce as a competitive differentiator. The company analyzes the cost of transitioning to an organic environment and determines that significant investment will be required, which may threaten the financial performance objectives of the entity. Given the importance of maintaining financial performance, the organization chooses to abandon the strategy.

Categorizing Business Objectives

216. How an organization categorizes its business objectives is decided by management. Regardless of how they are categorized, they must align with business practices, products, geographies, or other organizational dimensions.

217. In some cases, organizations must adhere to external requirements that set out the manner in which business objectives are categorized for reporting purposes. For example, if an organization is required to report on its environmental risk assessment as part of its operating license, it will specifically include those requirements within it business objectives and in its reporting.

218. Organizations need to be careful not to confuse business objectives categories with risk categories. Risk categories relate to the shared or common groupings of risks that potentially impact those business objectives.

Setting Performance Measures and Targets

219. The organization sets targets to monitor the performance of the entity and support the achievement of the business objectives. For instance:
    - An asset management company seeks to achieve a return on investment (ROI) of 5% annually on its portfolio.
    - A restaurant targets on-line home delivery orders to be delivered within 40 minutes.
    - A call center endeavors to minimize missed calls to 2% of overall calls received.
220. These targets should align with the strategy and risk appetite.
221. By setting targets, the organization is able to influence the risk profile of the entity. An aggressive target may result in a greater risk profile for that business objective. For example, an organization may set aggressive growth targets that heighten the risks in execution. Conversely, an organization may set a more conservative growth target that will lower the risk of achieving the target, but may also result in the target no longer aligning with the achievement of the business objective.
222. As another example, consider again the asset management company from the list above that understands that an ROI of 5% will enable the entity to achieve its financial objectives. If it strives for a return of 7%, it would incur greater risk in execution. If it strives for 3%, which allows for a less aggressive risk profile, it will not achieve its broader financial objectives. (Identifying and assessing the risks to the achievement of the business objective and monitoring the appropriateness of the performance measures and targets are discussed in Chapter 8.)
223. Example 7.11 provides a more thorough example of business objectives considered at the entity, division, operating unit, and function levels, along with supporting targets. The example illustrates how business objectives increase in specificity as they cascade throughout the entity and at all levels.

Example 7.11: Sample Business Objectives by Level

	Business Objective	Performance Measure and Target
Business objectives (entity)	• Continue to develop new, innovative products that interest and excite consumers • Expand retail presence in the health food sector	• 8 products in R&D at all times • 5% growth year over year
Business objectives for North America (division)	• Increase shelf space in leading stores that share our core values • Continue to source products in local markets	• 7% increase in shelf space • 92% local source rate
Business objectives for Snacks (operating unit)	• Develop high-quality and safe snack products that exceed consumer expectations	• 4.8 out of 5 in customer satisfaction survey
Business objectives for Human Resources (function)	• Maintain favorable annual turnover of employees • Recruit and train product sales managers in the coming year	• Turnover less than 10% • Recruit 50 sales managers • 95% training rate for sales staff

Principle 11: Defines Acceptable Variation in Performance

The organization defines acceptable variation in performance relating to strategy and business objectives.

Understanding Acceptable Variation in Performance

224. Acceptable variation in performance, closely linked to risk appetite, is sometimes referred to as "risk tolerance." It describes the range of acceptable outcomes related to achieving a business objective within the risk appetite. It also provides an approach for measuring whether risks to the achievement of strategy and business objectives are acceptable or unacceptable.

225. Unlike risk appetite, which is broad, acceptable variation in performance is tactical and focused. That is, it should be expressed in measurable units (preferably in the same units as the business objectives), be applied to all business objectives, and be implemented throughout the entity. In setting acceptable variation in performance, the organization considers the relative importance of each business objective and strategy. For instance, for those objectives viewed as being highly important to achieving the entity's strategy, or where a strategy is highly important to the entity's mission and vision, the organization may wish to set a lower level of acceptable variation in performance.

226. Operating within acceptable variation in performance provides management with greater confidence that the entity remains within its risk appetite and provides a higher degree of comfort that the entity will achieve its business objectives.

Performance Measures and Acceptable Variation

227. Performance measures related to a business objective help confirm that actual performance is within an established acceptable variation in performance (see Example 7.12). Performance measures can be either quantitative or qualitative (see Example 7.13).

Example 7.12: Sample Statements of Acceptable Variation in Performance

Business Objective	Target	Acceptable Variation in Performance
Return on investment (ROI) for an asset manager	Target 5% annual return on its portfolio	3% to 7% annual return
On-line home delivery orders for a restaurant	Target delivery within 40 minutes	30- to 50-minute delivery time
Minimize missed calls from a call center	Target 2% of overall calls	1% to 5% of overall calls

Example 7.13: Sample Qualitative and Quantitative Measures

Quantitative Performance Measures	Qualitative Performance Measures
Airline Industry	
• Number of new destinations • Percent of seats occupied • Revenue per seat	• Customer satisfaction • Brand recognition
Agriculture	
• Number of crops chosen • Crop production volume	• Organic certifications • Environmental compliance
Oil and Gas	
• Barrels per day • Number of active wells • Number of safety incidents	• Environmental protection • Health and safety record
Non-profit health organization	
• Number of donors and amount of donations • Number of research projects sponsored • Number of counseling programs offered	• Donor satisfaction • Social media commentary
Governmental agency	
• Number of permits issued • Number of people assisted	• Social media commentary • Public satisfaction

228. Acceptable variation in performance also considers both exceeding and trailing variation, sometimes referred to as positive or negative variation. Note that exceeding and trailing variation is not always set at equal distances from the target.

229. The amount of exceeding and trailing variation depends on several factors. An established organization, for example, with a great deal of experience, may move exceeding and trailing variation closer to the target as it gains experience at managing to a lower level of variation. The entity's risk appetite is another factor: an entity with a lower risk appetite may prefer to have less performance variation compared to an entity with a greater risk appetite.

230. It is common for organizations to assume that exceeding variation in performance is a benefit, and trailing variation in performance is a risk. Exceeding a target does usually indicate efficiency or good performance, not simply that an opportunity is being exploited. But trailing a target does not necessarily mean failure: it depends on the organization's target and how variation is defined (see Example 7.14).

Example 7.14: Trailing Target Variation

231. A large beverage bottler sets a target of having no more than five lost-time incidents in a year on the bottling floor and sets the acceptable variation in performance as zero to seven incidents. The exceeding variation between five and seven represents greater incidents and potential for lost time and an increase in health and safety claims, which is a negative result for the entity. In contrast, the trailing variation up to five represents a benefit: fewer incidents of lost time and fewer health and safety claims. The organization also needs to consider the cost of striving for zero lost-time incidents. Sometimes the pursuit of benefits detracts from the achievement of other business objectives, which is why there may be a limit placed on a positive variance.

232. Organizations should also understand the relationship between cost and acceptable variation in performance so they can deal effectively with associated risk and opportunities. Typically, the narrower the acceptable variation in performance, the greater amount of resources required to operate within that level of performance. Consider airlines, for example, which track on-time arrivals and departures. An airline may decide to stop serving several airports because its on-time performance does not fit within the airline's revised (decreased) acceptable variation in performance. The airline would then need to weigh the cost implications of forgoing service revenue to realize a decreased variation in its performance target.

8. Risk in Execution

Chapter Summary

233. An organization identifies and assesses risks that may impact the achievement of the entity's strategy and business objectives. Risks are prioritized according to their severity and considering the entity's risk appetite. The organization then selects risk responses and monitors performance for change. The organization determines a portfolio view of the amount of risk the entity has assumed in the pursuit of its strategy and business objectives.

Principles Relating to Risk in Execution

12. **Identifies Risk in Execution**—The organization identifies risk in execution that impacts the achievement of business objectives.
13. **Assesses Severity of Risk**—The organization assesses the severity of risk.
14. **Prioritizes Risks**—The organization prioritizes risks as a basis for selecting responses to risks.
15. **Identifies and Selects Risk Responses**—The organization identifies and selects risk responses.
16. **Develops Portfolio View**—The organization develops and evaluates a portfolio view of risk.
17. **Assesses Risk in Execution**—The organization assesses operating performance results and considers risk.

Introduction

234. Creating, preserving, and realizing an entity's value is further enabled by identifying, assessing, and responding to risk that may impact the achievement of the entity's strategy and business objectives. Risks originating at a transactional level may prove to be as disruptive as those identified at the entity level. Risks may also affect one operating unit or the entity as a whole. Risks may be highly correlated with factors within the business context or with other risks. Further, risk responses may require significant investments in infrastructure or may be accepted as part of doing business. Because risk emanates from a variety of sources and requires a range of responses, the process of identifying, assessing, and responding is undertaken across the entity and at all levels.

235. This component of the Framework focuses on enterprise risk management practices that support the organization in making decisions and achieving strategy and business objectives. To that end, organizations use their operating model to develop a process that:

- Identifies new and emerging risks so that management can deploy risk responses in a timely manner.
- Assesses the severity of risk, with an understanding of how the risk may change depending on the level of the entity.
- Prioritizes risks, allowing management to optimize the allocation of resources in response to those risks.
- Identifies and selects responses to risk.
- Develops a portfolio view to enhance the ability for the organization to articulate the amount of risk assumed in the pursuit of strategy and business objectives.
- Monitors entity performance and identifies substantial changes in the performance or risk profile of the entity.

236. Figure 8.1 illustrates that this process is iterative, with the inputs in one step of the process typically being the outputs of the previous step. This process is performed across all levels and with responsibilities and accountabilities for appropriate enterprise risk management aligned with severity of the risk.

Figure 8.1: Linking Risk Assessment Processes, Inputs, Approaches, and Outputs

Process	Inputs	Types of Approaches	Outputs
Identifying risk	• Strategy and business objectives • Risk appetite and acceptable variation in performance • Business context	• Data tracking • Interviews • Facilitated workshops • Questionnaires and surveys • Process analysis • Leading indicators	• Risk universe
Assessing risk	• Risk universe • Risk severity measures	• Probabilistic modeling (e.g., value at risk) • Non-probabilistic modeling (e.g., sensitivity analysis) • Judgmental evaluations • Benchmarking	• Risk assessment results

Figure 8.1 continued

Process	Inputs	Types of Approaches	Outputs
Prioritizing risk	• Risk assessment results • Prioritization criteria	• Judgmental evaluations • Quantitative scoring methods	• Prioritized risk assessment results
Responding to risk	• Prioritized risk assessment results	• Risk profile templates or pro forma risk profile • Cost benefit analysis	• Deployed risk responses • Residual risk assessment results
Developing a portfolio view	• Residual risk assessment results	• Judgmental evaluations • Quantitative scoring methods	• Portfolio view of risk
Monitoring performance	• Residual risk assessment results • Portfolio view of risk	• Dashboards • Performance Reports	• Corrective actions

Principle 12: Identifies Risk in Execution

The organization identifies risk in execution that impacts the achievement of business objectives.

Identifying Risk

237. The organization identifies new, emerging, and changing risks to the achievement of its strategy and business objectives. Organizations undertaking the risk identification process for the first time need to establish an inventory of risks and then, in subsequent identification processes, confirm existing risks as being still applicable and relevant. How often an organization goes through this process will depend on how quickly new risks emerge. Where risks are likely to take months or years to materialize, the frequency at which risk identification occurs may be less than where risks are less predictable or may occur at a greater speed.

238. New, emerging, and changing risks include those that:

- Arise from a change in business objectives (e.g., the entity adopts a new strategy supported by business objectives or amends an existing business objective).
- Arise from a change in business context (e.g., changes in consumer preferences for environmentally friendly or organic products that have potentially adverse impacts on the sales of the company's products).
- Pertain to a change in business context that may not have applied to the entity previously (e.g., a change in regulations that results in new obligations to the entity).
- Were previously unknown (e.g., the discovery of a susceptibility for corrosion in raw materials used in the company's manufacturing process).
- Have been previously identified but have since been altered due to a change in the business context, risk appetite, or supporting assumptions.

239. Management acknowledges that some risks may remain unknown—risks for which there could not have been reasonable expectation that they would have been considered in the risk identification process. These risks typically relate to changes in the business context. For example, the future actions or intentions of competitors are often unknown, but they may represent new risks to the performance of the entity.

240. Emerging risks also arise when business context changes, and they may alter the entity's risk profile in the future. Note that emerging risks may not be understood well enough to identify and assess accurately when they are first identified.

241. Identifying new and emerging risks, or changes in existing risks, allows management to look to the future and gives them time to assess the potential severity of the risks. In turn, having time to assess the risk allows management to anticipate the risk response, or to review the entity's strategy and business objectives as necessary.

242. Organizations want to identify those risks that are likely to disrupt operations and impact the reasonable expectation of achieving strategy and business objectives. Such risks represent significant change in the risk profile and may be either specific events or evolving circumstances. The following are some examples:

    - *Emerging technology:* Advances in technology that may impact the relevance and longevity of existing products and services.
    - *Expanding role of big data:* How organizations can effectively and efficiently access and transform large volumes of structured and unstructured data.
    - *Depleting natural resources:* The diminishing availability and increasing cost of natural resources that impact the supply, demand, and location for products and services.
    - *Rise of virtual entities:* The growing prominence of virtual entities that influence the supply, demand, and distribution channels of traditional market structures.
    - *Mobility of workforces:* Mobile and remote workforces that introduce new processes to the day-to-day operations of an entity.
    - *Labor shortages:* The challenges of securing labor with the skills and levels of education required by entities to support performance.
    - *Shifts in lifestyle, healthcare, and demographics:* The changing habits and needs of current and future customers as populations change.

243. When identifying risks, the organization should strive to be precise in wording, being sure to articulate the difference between an actual risk and other considerations, those being:

    - Potential root causes that could influence the severity of a risk.
    - Potential impacts of a risk being embedded in the description.
    - Potential impacts of ineffective or failed risk responses and controls.

244. Figure 8.2 provides some examples.

Figure 8.2: Describing Risks with Precision

Considerations Other than Risk	Risk Descriptions Illustrating Considerations Other than Risk	Preferred Risk Descriptions
Potential root causes	• Lack of training increases the risk that processing errors and incidents occur • Low staff moral contributes to the risk that key employees leave creating high turnover	• The risk that processing errors impact the quality of manufacturing units • The risk of losing key employees and turnover, impacting staff retention targets
Potential impacts of a risk being embedded in the description	• Production capacity fails to keep up with increased demand, and customer orders fall by 10% • Extreme weather creates a 20% higher -than-expected demand	• The risk that production capacity is unable to meet increased demand affecting production targets • The risk that higher-than-forecasted temperatures increase demand for summer products beyond capacity
Potential impacts of ineffective or failed risks	• The risk that bank reconciliations fail to identify incorrect payments to customers • The risk that quality assurance checks fail to detect product defects prior to distribution	• The risk of incorrect payments to customers impacting the entity's financial results • The risk of product defects impacting quality and safety goals

245. Accordingly, organizations are encouraged to describe risks by using a standard sentence structure. Here are two approaches:

- The possibility of [*describe potential occurrence or circumstance*] and the associated impacts on [*describe specific business objectives set by the organization*].
  - **Example**: The possibility of a change in foreign exchange rates and the associated impacts on revenue.
- The risk to [*describe the category set by the organization*] relating to [*describe the possible occurrence or circumstance*] and [*describe the related impact*].
  - **Example**: The risk to financial performance relating to a possible change in foreign exchange rates and the impact on revenue.

246. Precise risk identification is important because:

- It allows management to more accurately assess the severity of the risk.
- It helps management identify the typical root causes and impacts, and therefore select and deploy the most appropriate risk response.
- It supports the aggregation of risks to produce the portfolio view.

The Scope of Identification

247. Risk identification should occur at all levels: entity, division, operating unit, function, and process (see Example 8.1).

Example 8.1: Scope of Risk Identification

248. A regional energy company may identify risks associated with changes in the economic outlook at a division or entity level, but not at the process level. Conversely, it may identify the risk that a customer deadline may be missed at a process level, but not at the division or entity level. Regardless of where risks are identified, all risks form part of the entity's risk universe.

249. To demonstrate that risk identification is comprehensive, management will assess risk across all functions and levels—those that are common across more than one function, as well as those that are unique to a particular product, service offering, jurisdiction, or other function. Management must also account for risks that may exist beyond the immediate scope of a function. For example, the technology team of an entity may identify IT system and application-related risks, but those risks also impact other operating units. In this case, management identifies and confirms the appropriate risk owner.

Approaches to Risk Identification

250. A variety of approaches are available for identifying risks. These range from simple questionnaires to sophisticated facilitated workshops and meetings. Some approaches may be enabled by technology, such as on-line surveys, data tracking, and complex analytics.

251. Depending on the size, geographic footprint, and complexity of an entity, management may use more than one technique. For example, a larger entity may collect internal data on historical incidents and losses and analyze it to identify new, emerging, and changing risks. Some organizations may draw on information from other organizations in the same industry or region to inform them of potential risks. Figure 8.3 and the list below provide information on useful approaches for different types of risks.

Figure 8.3: Approaches for Identifying Risks

Type of Risk	Workshops	Interviews	Process Analysis	Key Risk Indicators	Data Tracking
Existing	✓	✓	✓	✓	✓
New	✓	✓	✓		✓
Emerging	✓	✓			✓

- *Workshops* bring together individuals from different functions and levels to draw on the group's collective knowledge and develop a list of risks as they relate to the entity's strategy or business objectives.
- *Interviews* solicit the individual's knowledge of past and potential events. For canvassing large groups of people, questionnaires or surveys may be used.
- *Process analysis* involves developing a diagram of the process to better understand the interrelationships of its component inputs, tasks, outputs, and responsibilities. Once mapped, risks can be identified and considered against relevant business objectives.

- *Key risk indicators* are qualitative or quantitative measures designed to identify changes to existing risks. Risk indicators should not be confused with performance measures, which are typically retrospective in nature.
- Data tracking from past events can help predict future occurrences. While historical data typically is used in risk assessment—based on actual experience with severity—it can also be used to understand interdependencies and develop predictive and causal models. Databases developed and maintained by third-party service providers that collect information on incidents and losses incurred by industry or region may inform the organization of potential risks. These are often available on a subscription basis. In some industries, consortiums have formed to share internal data.

252. Whatever approaches are selected, management considers how changes in assumptions underpinning the strategy and business objectives may create new or emerging risks. Management may wish to consider the expected economic outlook for the entity, changing customer preferences, shifts in planned product profitability, and anticipated growth rates.

Identifying Potential Opportunities

253. Inherent in identifying risk is identifying opportunities. That is, sometimes opportunities emerge from risk. For example, changes in demographics and aging populations may be considered as both a risk to the current strategy of an entity and an opportunity for growth. Similarly, advances in technology may represent a threat to current distribution and service models for retailers as well as an opportunity to change how retail customers obtain goods (e.g., through on-line services). Where such opportunities are identified, they are communicated back to management to consider as part of strategy and business objective-setting.

Risk Universe

254. The risks captured by the risk identification process are commonly referred to as a risk universe— a qualitative listing of the risk the entity faces. Depending on the number of individual risks identified, organizations may structure the risk universe using a specific taxonomy, or hierarchy of risk types, which provides standard definitions and categories for different risks. This allows organizations to group similar risks together, such as strategic, financial, operational, and compliance risks. Within each category, organizations may choose to further define risks into more detailed sub-categories. The risk universe can be updated to reflect the changes identified by management.

Principle 13: Assesses Severity of Risk

The organization assesses the severity of risk.

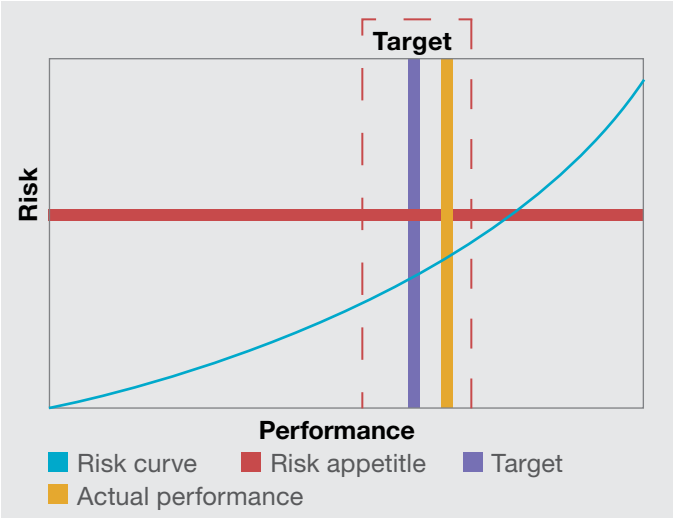
Assessing Risk

255. The risks identified and included in an entity's risk universe are assessed in order to understand the severity of each risk to the achievement of an entity's strategy and business objectives. The risk universe forms the basis from which an organization is able to construct a risk profile (Figure 8.4).

256. Management may use the risk profile in its assessment to:

- Confirm that performance is within the acceptable variation in performance.
- Confirm that risk is within risk appetite.
- Compare the severity of a risk at various points of the curve.
- Assess the disruption point in the curve, at which the amount of risk greatly exceeds the appetite of the entity and impacts its performance or the achievement of its strategy and business objectives.

Figure 8.4: Risk Profile



257. In addition, management considers how different risks may present different impacts to the same business objective. For example, a hardware store franchise identifies the risk of not stocking a diverse product range that will appeal to a broad group of customers, which will impact sales growth. The stores are all located in the same region. Analysis of the sales history reveals a strong positive correlation to the prevailing economic conditions. Management identifies that the risk of a downturn in the region's economy would adversely impact sales growth for the entire franchise, regardless of the products in stock.

Assessing Severity at Different Levels of the Entity

258. The severity of risk is assessed at multiple levels of the entity as it will not be the same across divisions, functions, and operating units. For example, risks that are assessed as important at the operating unit level may be less important at a division or entity level. In the more senior levels of the entity, risks are likely to have a greater impact on reputation, brand, and trustworthiness.

259. Risk assessment employs a taxonomy to group common risks. For example, the risk of technology disruptions identified by multiple operating units may be grouped and assessed collectively. Similarly, the risks measured at more senior levels within an entity may also be grouped. When common risks are grouped, the severity rating may change. Risks that are of low severity individually may become more or less severe when considered collectively across operating units or divisions.

Assessment Approaches

260. Risk assessment approaches may be qualitative, quantitative, or both. The anticipated severity of a risk may influence the type of approach used. Types of approaches include scenario analysis, simulation, data analysis, and interviews, among others.

261. In assessing risks that could have extreme impacts, management may use scenario analysis, but when assessing the effects of multiple events, management might find simulations more useful. Conversely, high-frequency, low-impact risks may be more suited to data analysis. To reach consensus on the severity of risk, organizations may employ the same approach they used as part of the risk identification, such as workshops and interviews.

262. Qualitative assessment approaches are often used where risks do not lend themselves to quantification or when it is neither practicable nor cost effective to obtain sufficient data for quantification. 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). To assess other types of risk, management may use a combination of data, benchmarking information, and expertise.

263. Assessments may also be performed across the entity by different teams. In this case, the organization establishes a process to review any differences in the assessment results. For example, if one team rates particular risks as "low," but another team rates them as "medium," management reviews the results to determine if there are inconsistencies in approach, assumptions, and perspectives of business objectives or risks.

Inherent, Target, and Residual Risk

264. Management considers inherent risk, target residual risk, and actual residual risk as part of the risk assessment.

- *Inherent risk* is the risk to an entity in the absence of any direct or focused actions by management to alter its severity.
- *Target residual risk* is the amount of risk that an entity prefers to assume in the pursuit of its strategy and business objectives, knowing that management will implement, or has implemented, direct or focused actions by management to alter risk severity.
- *Actual residual risk* is the risk remaining after management has taken action to alter its severity. Actual residual risk should be equal to or less than the target residual risk, as is illustrated in Figure 8.5. Where actual residual risk exceeds target risk, additional actions should be identified that allow management to alter risk severity further.

Figure 8.5: Inherent, Target, and Residual Risk

265. Even when actual residual risk is assessed to be within target residual risk, management may wish to identify opportunities that can move the entity closer to the desired residual risk profile (see Example 8.2).

Example 8.2: Target and Residual Risk

266. A small advertising company moves to an automated workflow approval system in order to reduce the risk of version control and documentation errors in client materials. While the existing manual process has mitigated the risk to within its target residual risk range, the automated workflow system now offers an additional risk response to further reduce the risk, and does so in a more cost-effective manner.

267. Alternatively, management may identify risks for which unnecessary responses have been deployed. Redundant risk responses are those that do not result in a measurable change to the severity of the risk. Removing such responses may allow management to allocate resources put toward that response elsewhere.

Selecting Severity Measures

268. Risk emanates from multiple sources and results in different impacts. Figure 8.6 illustrates the variety of results that may occur from a variety of sources.

Figure 8.6: Causes and Impacts of Risk

269. When assessing risks, management must consider potential causes of different risks and the consequent severity of any impacts. For example, when a software developer assessed the risk of a variance in sales for a new product on the division's sales targets, it determined the causes of the risk included issues with software production, understanding customer preferences, or a launch strategy that proved to be more successful than expected. The impact of the risk—a variance in sales—may result in financial targets not being achieved, the inability to fulfill increased customer orders, and an overall deterioration in the entity's reputation.

270. The measures used to assess the severity of risk are aligned to the size, nature, and complexity of the entity and its risk appetite. Different measures may also be used at varying levels of an entity for which a risk is being assessed. The thresholds used to assess the severity of a risk may be tailored to the level of assessment—by entity or operational unit. Acceptable amounts of financial risk, for example, may be greater if those risks are assessed at an entity level compared to an operating unit.

271. The severity of the risk is determined by management in order to select an appropriate risk response, allocate resources, and support management decision-making and performance. Measures may include:[20]

- *Impact*: Result or effect of a risk. There may be a range of possible impacts associated with a risk. The impact of a risk may be positive or negative relative to the strategy or business objectives.

20 Additional measures, including persistence, velocity, and complexity, are discussed in Principle 14.

- *Likelihood*: The possibility of a risk occurring. This may be expressed in a variety of ways:
  - **Example of qualitative description:** "The possibility of a risk relating to a potential occurrence or circumstance and the associated impacts on a specific business objective [within the time horizon contemplated by the business objective, e.g., 12 months] is remote."
  - **Example of quantitative description:** "The possibility of a risk relating to a potential occurrence or circumstance and the associated impacts on a specific business objective [within the time horizon contemplated by the business objective, e.g., 12 months] is 80%."
  - **Example of frequency:** "The possibility of the risk relating to a potential occurrence or circumstance and the associated impacts on a specific business objective [within the time horizon contemplated by the business objective, e.g., 12 months] is once every 12 months."

272. The time horizon used to assess risks should be the same as that used for the related strategy and business objectives. Because the strategy and business objectives of many entities focus on short- to medium-term time horizons, management often focuses on risks associated with those time frames. Specifically, when assessing risks of the mission, vision, or strategy, some aspects may be longer term. As a result, management needs to be cognizant of the longer time frames and not ignore risks that might emerge or occur further out.

273. Severity measures should align with the risk, strategy, and business objectives. Consider the example of the snack food company described in Principle 10 (Example 7.11). The organization identifies the risks to its business objectives (see Example 8.3) and then applies the appropriate measure. Management provides guidance on how to assess the severity of the impact where different impacts are identified. Where multiple impacts result in different assessments of severity or require a different risk response, management determines if additional risks need to be identified and assessed separately.

Example 8.3: Mapping Business Objectives, Risk, and Severity Measures

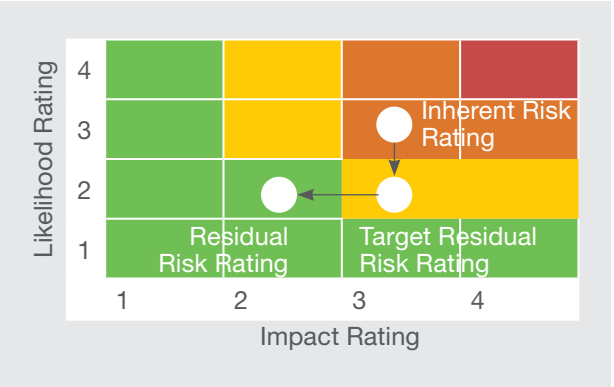
Objective Type	Business Objectives and Target	Identified Risk	Acceptable Variation in Performance	Severity Measure (Impact)
Business objectives for Snacks (operating unit)	Continue to develop new, innovative products that interest and excite consumers. Target: 8 products in R&D at all times	Relating to new products, the entity fails to develop new snacks that exceed customer expectations	Expected growth of new snack products in development of 6 to 12 at all times	Financial impacts
Business objectives for Human Resources (function)	Recruit and train product sales managers in the coming year Target: recruit 50 product sales managers and train 95% of sales managers	Relating to the recruitment of product sales managers, the entity is unable to identify appropriately qualified people	The entity recruits between 35 and 50 product managers in the coming year	Operational/ HR impacts
		Relating to the training of product sales managers, the entity is unable to schedule training that accommodates new hires availability and physical location	The entity trains a minimum of 85% of product sales managers in the coming year	

Depicting Residual Risk

274. Assessment results are often depicted using a "heat map" or other graphical representation to highlight the relative severity of each of the risks to the achievement of a given strategy or business objective. On the heat map shown in Figure 8.7, arrows represent the desired direction of risk as the entity progressively reduces the severity of the risk. Each risk plotted on the heat map assumes a given level of performance for that strategy or business objective. A heat map does not account for changes in performance that may result in a change in the severity of identified risks.

275. Identified risks are plotted on the heat map using the severity measures selected by the entity. The color coding aligns to a particular severity outcome and reflects the risk appetite of the entity. In Figure 8.7, the entity has four risk severity ratings. The various combinations of likelihood and impact (severity measures), given the risk appetite, are color coded to reflect a particular level of severity. More risk-averse entities will account for a larger number of outcomes, color coded as red, compared to less risk-averse entities. Less risk-averse entities may have a more balanced distribution of potential severity outcomes.

Figure 8.7: Heat Map



Other Considerations

276. Part of the identification process is seeking to understand the interdependencies that may exist between risks. Interdependencies can occur where multiple risks affect one business objective or where one risk triggers another. Risks can occur concurrently or sequentially. For example, for a technology innovator the delay in launching new technology products results in a concurrent loss of market share and dilution of the entity's brand value. How management understands interdependencies will be reflected in the assessment of severity.

277. The organization strives to identify triggers that will prompt a reassessment of severity when required. Triggers are typically changes in the business context, but may also be changes in the risk appetite. The organization selects triggers that help demonstrate the sensitivity of a risk to a change in the business context or that can act as an early warning indicator of changes to assumptions underpinning the severity assessment. Examples of triggers include an increase in the number of customer complaints, an adverse change in an economic index, a drop in sales, or a spike in employee turnover. The severity of the risks and the frequency at which severity may change will inform how often the assessment may be triggered. For example, risks associated with changing commodity prices may need to be assessed daily, but risks associated with changing demographics or market tastes for new products may need to be assessed only annually.

Bias in Assessment

278. Management should identify and mitigate the effect of bias in the assessment process. Bias may result in the severity of a risk being under- or overestimated, and limit how effective the selected risk response will be. Overestimating risks may result in resources being unnecessarily deployed in response, creating inefficiencies in the entity. Overestimating severity may also hamper the performance of the entity or affect its ability to identify new opportunities. Underestimating the severity of a risk may result in an inadequate response, leaving the entity exposed and at risk potentially outside of the entity's risk appetite.

Principle 14: Prioritizes Risks

The organization prioritizes risks as a basis for selecting responses to risks.

Establishing the Criteria

279. Organizations prioritize risks in order to inform decision-making and optimize the allocation of resources. Risk prioritization considers the severity of a risk and informs the selection of the risk response. The priorities are determined by applying agreed-upon criteria.[21] Examples of these criteria include:

- *Adaptability*: The capacity of an entity to adapt and respond to risks (e.g., responding to changing demographics such as the age of the population).
- *Complexity*: The scope and nature of a risk to the entity's success. The interdependency of risks will typically increase their complexity.
- *Velocity*: The speed of onset at which a risk impacts an entity. The velocity may move the entity away from the acceptable variation in performance.
- *Persistence*: How long a risk impacts an entity (e.g., accounting for the immediacy of disrupted operations compared to the longer-term impact to the entity's reputation).
- *Recovery*: The capacity of an entity to return to acceptable variation in performance (e.g., continuing to function after a severe flood or other natural disaster). Recovery excludes the time taken to return to acceptable variation in performance, which is considered part of persistence, not part of recovery.

280. Prioritization also takes into account the severity of the risk compared to risk appetite. Greater priority may be given to those risks that are more likely to approach or exceed risk appetite.

Prioritizing Risk

281. The criteria for prioritizing risk are applied to assessed risks in order to identify and select risk responses. Note that risks with similar assessments of severity may be prioritized differently. That is, two risks may both be assessed as "high," but management may give one more priority because it has greater velocity and persistence (see Example 8.4).

Example 8.4: Prioritizing Risk

282. For a large restaurant chain, responding to the risk that customer complaints remain unresolved and attract adverse coverage in social media may be considered a greater priority than responding to the risk that contract negotiations with vendors and suppliers are protracted. Both risks are severe, but the speed and scope of on-line scrutiny may have a greater impact on the performance and reputation of the restaurant chain, necessitating a quicker response to negative feedback.

283. How a risk is prioritized typically informs the risk responses management considers. The most effective responses address both severity (impact and likelihood) and prioritization (velocity, complexity, etc.).

21 Note that the criteria may also be used as measures to assess the severity of a risk as discussed in Principle 13.

284. Prioritization ultimately supports the portfolio view of risk. Risks of greater priority are more likely to be those that affect the entity as a whole or arise at the entity level. For example, the risk that new competitors will introduce new products and services to the market may require greater adaptability and a review of the entity's strategy and business objectives in order for the entity to remain viable and relevant.

Using Risk Appetite to Prioritize Risks

285. Comparing risk profile to risk appetite helps when setting priorities. Risks that result in the entity approaching the acceptable variation in performance or risk appetite for a specific business objective are typically given higher priority (see Example 8.5).

Example 8.5: Relationship of Risk Profile to Risk Appetite

286. A utility company's mission is to be the most reliable electricity provider in its region. A recent increase in the frequency and persistence of power outages indicates that the company is approaching its risk appetite and is therefore less likely to achieve its business objectives. This situation triggers a heightened priority for the risk. A change in the priority may result in reviewing the risk response, implementing additional responses, and allocating more resources to reduce the likelihood of the risk breaching the organization's risk appetite.

287. Through the process of prioritizing risks, management also recognizes that there are risks the entity chooses to accept; that is, some are already considered to be managed to an acceptable amount for the entity and for which no additional risk response will be contemplated.

Prioritization at All Levels

288. Risk prioritization occurs at all levels of an entity, and different risks may be assigned different priorities at different levels. For example, high-priority risks at the operating level may be low-priority risks at the entity level. The organization assigns a priority at the level at which the risk is owned and with those who are accountable for managing it.

289. Risk owners are responsible for using the assigned priority to select and apply appropriate risk responses. In many cases, the risk response owner and risk owner may be two different people, or may be at different levels within the entity. Risk owners must have sufficient authority to prioritize risks based on their responsibilities and accountability for managing the risk effectively.

290. Organizations prioritize risks on an aggregate basis where a single risk owner is identified or a common risk response is likely to be applied. This allows risks to be clearly identified and described using a standard risk taxonomy, which enables common risks to be prioritized consistently across the entity. For example, several operating units across an entity have identified the risk of technology failures. Using a standard taxonomy, the risks are grouped and prioritized on an aggregate basis. The result is a more consistent and efficient risk response than would have occurred if each risk had been prioritized separately.

Recognizing Bias

291. Management must strive to prioritize risks and manage competing business objectives relating to the allocation of resources free from bias. Competing business objectives may include securing additional resources, achieving specific performance measures, qualifying for personal incentives and rewards, or obtaining other specific outcomes. The prevalence of bias may increase in situations where there are competing priorities.

Principle 15: Identifies and Selects Risk Responses

The organization identifies and selects risk responses.

Choosing Risk Responses

292. For all risks identified, management selects and deploys a risk response. Risk responses fall within the following categories:

- *Accept*: No action is taken to affect the severity of the risk. This response is appropriate when the risk is already within risk appetite. A risk that is outside the entity's risk appetite and that management seeks to accept will generally require approval from the board or other oversight bodies.
- *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 was not able to identify a response that would reduce the impact of the risk to an acceptable amount of severity.
- *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.
- *Reduce*: Action is taken to reduce the severity of the risk. This involves any of myriad everyday business decisions that reduces residual risk to an amount of severity aligned with the target residual risk profile and risk appetite.
- *Share*: Action is taken to reduce the severity of the 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.

293. When an organization chooses "avoid" as the response to risk, it is taking action to remove the risk to the achievement of strategy and business objectives. The decision to avoid a strategy or business objective in favor of one of the other alternatives is considered part of the strategy-setting process, but that decision may introduce new risks to the entity's strategy and business objectives.

294. These categories of risk responses assume that the risk can be managed within the organization's risk appetite and within an acceptable variation in performance. In some instances, management may need to consider another course of action, including the following:

- *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. As with a review of business objectives, this may occur when other categories of risk responses do not represent desired courses of action for the entity.

295. Organizations may also choose to exceed the risk appetite if the effect of staying within the appetite is perceived to be greater than the potential exposure from exceeding it. For example, management may accept the risks associated with the expedited approval of new products in favor of the opportunities and competitive advantage of bringing those products to market more quickly. Where an entity repeatedly accepts risks that approach or exceed appetite as part of its usual operations, a review and recalibration of the risk appetite may be warranted.

Selecting and Deploying Risk Responses

296. Management selects and deploys risk responses while considering the following factors:

- *Business context*: Risk responses are selected or tailored to the industry, geographic footprint, regulatory environment, operating model, or other factors.
- *Costs and benefits*: Anticipated costs and benefits are generally commensurate with the severity and prioritization of the risk.
- *Obligations and expectations*: Risk response addresses generally accepted industry standards, stakeholder expectations, and alignment with the mission and vision of the entity.
- *Risk priority*: The priority assigned to the risk informs the allocation of resources. Risk reduction responses that have large implementation costs (e.g., system upgrades, increases in personnel) for lower-priority risks need to be carefully considered and may not be appropriate given the assessed severity.
- *Risk severity*: Risk response should reflect the size, scope, and nature of the risk and its impact on the entity. For example, in a transaction or production environment, where risks are driven by changes in volume, the proposed response is scaled to accommodate increased activity.
- *Risk appetite*: Risk response either brings risk within risk appetite of the entity or maintains its current status. Management identifies the response that brings residual risk to within the appetite. This may be, for example, a combination of purchasing insurance and implementing internal responses to reduce the risk to an acceptable variation in performance.

297. Often, any one of several risk responses will bring the residual risk in line with the acceptable variation in performance, and sometimes a combination of responses provides the optimum result. Conversely, sometimes one response will affect multiple risks, in which case management may decide that additional actions to address a particular risk are not needed.

298. The risk response may change the risk profile. For example, fruit farmers may purchase weather-related insurance for floods or storms that would result in production levels dropping below a certain minimum volume. The risk profile for production levels would account for the potential performance outcomes covered by insurance.

299. Once management selects a risk response, control activities[22] are necessary to ensure that those risk responses are executed as intended. Management must recognize that risk is managed but not eliminated. Some residual risk will always exist, not only because resources are limited, but because of future uncertainty and limitations inherent in all tasks.

22 Control activities are discussed in *Internal Control—Integrated Framework*.

Considering Costs and Benefits of Risk Responses

300. Management must consider the potential costs and benefits of a risk response. Generally, anticipated costs and benefits are commensurate with the severity and prioritization of the risk. Cost and benefit measurements for selecting and deploying risk responses are made with varying levels of precision. Costs comprise direct costs, indirect costs (where practicably measurable), and for some entities, opportunity costs associated with the use of resources. Measuring benefits may be more subjective, as they are usually difficult to quantify. In many cases, however, the benefit of a risk response can be evaluated in the context of the achievement of strategy and business objectives. In some instances, given the importance of a strategy or business objective, there may not be an optimal risk response from the perspective of costs and benefits. In such instances, the organization can either select a response or choose to revisit the entity's strategy and business objectives.

301. Management is also responsible for risk responses that address any regulatory obligations, which again may not be optimal from the perspective of costs and benefits, but comply with legal or other obligations (see Example 8.6). In selecting the appropriate response, management must consider the expectations of stakeholders such as shareholders, regulators, and customers.

Example 8.6: Considering Regulatory Requirements when Choosing Risk Responses

302. A regional insurance company implements risk responses to address new regulatory requirements across the insurance industry. These responses will require the company to make additional investments in its technology infrastructure, change in its current processes, and add to its staff to assist with the implementation.

Additional Considerations

303. Selecting one risk response may introduce new risks that have not previously been identified or may have unintended consequences. For newly identified risks, management should assess the severity and related priority, and determine the effectiveness of the proposed risk response. On the other hand, selecting a risk response may present new opportunities not previously considered. Management may identify innovative responses, which, while fitting with the response categories described earlier, may be entirely new to the entity or even an industry. Such opportunities may surface when existing risk response options reach the limit of effectiveness, and when further refinements likely will provide only marginal changes to the severity of a risk. Management channels any new opportunities back to the strategy-planning process.

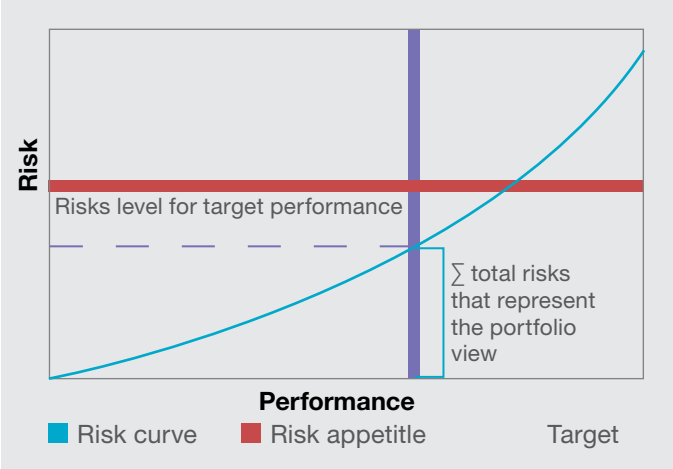
Principle 16: Develops Portfolio View

The organization develops and evaluates a portfolio view of risk.

Understanding a Portfolio View

304. Enterprise risk management requires the organization to consider potential implications to the risk profile from an entity-wide, or portfolio, perspective. Management first considers risk as it relates to each division, operating unit, or function. Each manager develops a composite assessment of risks that reflects the unit's residual risk profile relative to its business objectives and acceptable variation in performance.

Figure 8.8: Risk Profile Showing Risk as a Portfolio View



305. A portfolio view allows management and the board to consider the type, severity, and interdependencies of risks, and how they may affect performance. Using the portfolio view, the organization identifies risks that are severe at the entity level. These may include risks that arise at the entity level as well as transactional, processing-type risks that are severe enough to disrupt the entity as a whole. Figure 8.8 illustrates the portfolio view on a risk profile.

306. With a portfolio view, management is well positioned to determine whether the entity's residual risk profile aligns with the overall risk appetite. The same risk across different units may be acceptable for the operating units, but taken together may give a different picture. Collectively, the risk may exceed the risk appetite of the entity as a whole, in which case additional or different risk responses are needed. Conversely, a risk may not be acceptable in one unit, but well within the range in another. For example, some operating units have higher risk than others, which results in overall risk falling within the entity's risk appetite. And in cases where the portfolio view shows that risks are significantly less than the entity's risk appetite, management may decide to motivate individual operating unit managers to accept greater risk in targeted areas, striving to enhance the entity's overall growth and return.

Developing a Portfolio View

307. A portfolio view of risk can be developed in a variety of ways. One method is to focus on major risk categories across operating units, or on risk for the entity as a whole, using metrics such as risk-adjusted capital or capital at risk. This method is particularly useful when assessing risk against business objectives stated in terms of earnings, growth, and other performance measures, sometimes relative to allocated or available capital. The information derived can prove useful in reallocating capital across operating units and modifying strategic direction.

308. A portfolio view also may be depicted graphically indicating the types and amount of risk assumed compared to the risk appetite of the entity for each organizational function, strategy, and business objective.

309. In developing the portfolio view, organizations may observe risks that:
    - Increase in severity as they are progressively consolidated to higher levels within the entity.
    - Decrease in severity as they are progressively consolidated.
    - Offset other risks by acting as natural hedges.

Analyzing the Portfolio View

310. To evaluate the portfolio view of risk, the organization will want to use both qualitative and quantitative techniques. Quantitative techniques include regression modeling and other means of statistical analysis to understand the sensitivity of the portfolio to changes and shocks. Qualitative techniques include scenario analysis and benchmarking.
311. By stressing the portfolio, management can review:
    - Assumptions underpinning the assessment of the severity of risk.
    - Behaviors of individual risks under stressed conditions.
    - Interdependencies of risks within the portfolio view.
    - Effectiveness of existing risk responses.
312. Undertaking stress testing, scenario analysis, or other analytical exercises helps an organization to avoid or better respond to big surprises and losses. The organization uses different techniques to assess the effect of changes in the business context or other variables on a business objective or strategy. For example, an organization may choose to analyze the effect of a change in interest rates on the portfolio view. Alternatively, the organization may seek to understand the impact of multiple variables occurring concurrently, such as changing interest rates combined with a spike in commodity prices that impact the entity's profitability. Finally, the organization may choose to evaluate the impact of a large-scale event, such as an operational incident or third-party failure. 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.
313. The purpose of these exercises is to assess the adaptive capacity of the entity. Techniques also invite management to challenge the assumptions underpinning the selection of the entity's strategy and assessment of the risk profile. As such, analysis of the portfolio view can also form part of an organization's evaluation in selecting a strategy or establishing business objectives.

Principle 17: Assesses Risk in Execution

The organization assesses operating performance and considers risk.

Monitoring Entity Performance

314. Organizations review entity performance to determine how risk has manifested and impacted strategy and business objectives compared to the risk appetite of the entity. As noted in Chapter 7, Risk, Strategy, and Objective-Setting, management considers the relative importance of each business objective and aligns each with the acceptable variation in performance with risk appetite. Knowing that the entity is operating within acceptable variation and risk appetite provides management with a higher degree of confidence that the entity will achieve its business objectives.

315. By monitoring performance, organizations seek answers to these questions:

- **Has the entity performed as expected and achieved its target?** The organization identifies variances that have occurred and considers what may have contributed to them. For example, consider an entity that has committed to opening five new office locations every year to support its longer-term growth strategy to build a presence across the country. The organization has determined that it could continue to achieve its strategy with only three offices opening, and would be taking on more risk than desired if it opened seven or more offices. The organization therefore monitors performance and determines whether the entity has opened the expected number of offices, and how those new offices are performing. If the growth is below plan, the organization may need to revisit the strategy.
- **What risks are occurring that may be affecting performance?** Monitoring confirms whether risks were previously identified, or whether new, emerging risks have occurred. For example, monitoring helps confirm that the risk of delays due to additional permit requirements for construction did occur and affected the number of new offices opened.
- **Was the entity taking enough risk to attain its target?** Where an entity has failed to meet its target, the organization needs to determine if the failure is due to risks that are impacting the achievement of the target or insufficient risk being taken to support the achievement of the target. Using the same example, suppose the entity opens only three offices. In this case management observes that the planning and logistics teams are operating below capacity and that other resources set aside to support the opening of new offices have remained unused. Insufficient risk was taken by the entity despite having allocated resources.
- **Was the estimate of the amount of risk accurate?** When risk has not been assessed accurately, the organization asks why. To answer that question, the organization must challenge the understanding of the business context and the assumptions underpinning the initial assessment. It must also determine whether new information has become available that would help refine the assessment. For example, suppose the example entity opens five offices and observes that the estimated amount of risk was too low compared to the types and amount of risk that have occurred.

316. If an organization determines that performance does not fall within its acceptable variation, or that the target performance results in a different risk profile than what was expected, it may need to:

- *Review business objective or strategy*: An organization may choose to change or abandon a business objective if the performance of the entity is not achieved within acceptable variation.
- *Review strategy*: Should the performance of the entity result in a substantial deviation from the expected risk profile, the organization may choose to revise its strategy. In this case, it may choose to reconsider alternative strategies that were previously evaluated, or identify new strategies.
- *Revise target performance*: An organization may choose to revise the target performance level to reflect a better understanding of the reasonableness of potential performance outcomes and the corresponding severity of risks to the business objective.
- *Severity of risk results*: An organization may re-perform the risk assessment for relevant risks, and results may alter based on changes in the business context, the availability of new data or information that enables a more accurate assessment, or challenges to the assumptions underpinning the initial assessment.
- *Review how risks are prioritized*: An organization may take the opportunity to either raise or lower the priority of identified risks to support reallocating resources. The change reflects a revised assessment of the prioritization criteria previously applied.

- *Revise risk responses*: An organization may consider altering or adding responses to bring risk in line with the target performance and risk profile. For risks that are reduced in severity, an organization may redeploy resources to other risks or business objectives. For risks that increase in severity, the organization may bolster responses with additional processes, people, infrastructure, or other resources.
- *Revise risk appetite*: Corrective actions are typically undertaken to maintain or restore the alignment of the risk profile with the entity's risk appetite, but can extend to revising it. However, this action requires review and approval by the board or other risk oversight body.

317. The extent of any corrective actions must align with the magnitude of the deviation in performance, the importance of the business objective, and the costs and benefits associated with altering risk responses. Consider, for example, a small retailer that stocks a significant portion of its inventory from local producers. The retailer monitors the financial results of its shop on a weekly basis and realizes locally produced goods are not sufficiently profitable to meet its financial goals. It therefore decides to revise its business objective of sourcing locally and begins to import less expensive goods to improve its financial performance. The retailer also recognizes that this change may affect other risks, such as logistics, currency fluctuations, and time to market.
318. Where monitoring repeatedly identifies new risks that were not identified through the organization's risk identification processes, or where the actual risk is inconsistent with severity ratings, management determines whether a review of enterprise risk management practices is warranted. A more detailed discussion on reviewing the risk assessment process can be found in Principle 23.

Considering Entity Capabilities

319. Part of monitoring performance is considering the organization's capabilities and their effect on performance. If performance targets are not being met, is it because there are insufficient capabilities? If targets are being exceeded, is it because corrective action is required? The organization must answer these questions.
320. Corrective action may include reallocating resources, revising business objectives, or exploring alternative strategies (see Example 8.7).

Example 8.7: Considering Entity Capabilities

321. For a local government, the economy is largely supported by tourism. City officials understand the minimum, targeted, and maximum levels of tourism required to support their financial objectives. Specifically, they determined how much income can be generated through tourism based on metrics such as hotel reservations and occupancy rates. They found that an occupancy rate of 50% (its target) would provide the city with enough revenue to support its annual operating budget and fund other programs. However, an occupancy rate greater than 85% would have an impact on the city's risk profile, creating risks relating to the usage of the public transportation system, incidents of disorderly conduct and crime, and the stress on the sanitation system. The city therefore monitors the performance of its tourism industry in order to make more risk-aware decisions on the aggressiveness of its future marketing campaigns and ensure that the capacity for tourism is managed.

322. The entity's capacity for resources also informs decisions for corrective actions. For business objectives that affect the entity as a whole, the organization may choose to revise the objective instead of incurring the costs of deploying additional risk responses. Whenever significant deviations from the acceptable variation in performance occur, or where performance represents a disruption to the achievement of the entity's strategy, the organization may revise its strategy.

9. Risk Information, Communication, and Reporting

Chapter Summary

323. Communication is the continual, iterative process of providing, sharing, and obtaining information, which flows throughout the entity. Management uses relevant information from both internal and external sources to support enterprise risk management. The organization leverages information systems to capture, process, and manage data and information. Using information applicable to all components, the organization reports on risk, culture, and performance.

Principles Relating to Information and Communication Channels

18. **Uses Relevant Information**—The organization uses information that supports enterprise risk management.
19. **Leverages Information Systems**—The organization leverages the entity's information systems to support enterprise risk management.
20. **Communicates Risk Information**—The organization uses communication channels to support enterprise risk management.
21. **Reports on Risk, Culture, and Performance**—The organization reports on risk, culture, and performance at multiple levels of and across the entity.

Introduction

324. Advances in technology and business have resulted in exponential growth in volume of and heightened attention on data. The enormous quantity of data, the speed at which it must be stored, and the wide variety of data types and sources present many challenges for organizations. Once data is processed, organized, and structured into information about a particular fact or circumstance, it becomes a source for knowledge. However, one main challenge is avoiding information overload. With so much data available—often in real time—to more people in an entity, it is important to provide the right information, in the right form, at the right level of detail, to the right people, at the right time.

325. "Data" is the collection of raw facts that can be analyzed, used, or referenced. Organizations transform data into information about stakeholders, products, markets, and competitor actions. Through their communication channels, they can provide timely, relevant information to targeted audiences.

326. An enterprise risk management taxonomy provides the basis for supporting risk data and information. An organization can implement this taxonomy structure into its information systems to consistently aggregate risk data and information. It is of great value to an organization to use an enterprise risk management taxonomy to identify and categorize risks that could affect the entity's strategy and business objectives.

Principle 18: Uses Relevant Information

The organization uses information to support enterprise risk management.

Putting Relevant Information to Use

327. Organizations leverage enterprise risk management to identify "relevant information," which is simply information that applies to making informed business decisions. With relevant information in hand, organizations can be more agile in their decision-making, giving them a competitive advantage. Organizations use information to anticipate situations that may impede the achievement of strategy and business objectives.

328. The process of identifying what information the organization may require to apply enterprise risk management practices is continual and specific to each component. Organizations consider what information is available to management (which may be more than is needed), and the cost of obtaining that information. Management and other personnel can then identify which sources of information are needed to support the components of enterprise risk management:

- As part of the component Risk Governance and Culture, management may need information on the standards of conduct and individual performance relative to those standards. For instance, professional service firms have specific standards of conduct to help maintain independent relationships with clients. Annual staff training reinforces those standards, and testing of staff knowledge provides management with relevant information on individuals' comprehension of their desired behaviors as they relate to the entity's independence.
- As part of the component Strategy and Objective-Setting, management may need information on stakeholder expectations of risk appetite. Stakeholders such as investors and customers may express their expectations through analyst calls, blog postings, contract terms and conditions, etc. These provide relevant information on the types and amount of risk an entity may be willing to accept and strategy they pursue.

- As part of the component Risk Identification, Assessment, and Response, management may need information on competitor actions to assess changing risk. For example, a large residential real estate company may assess the risk of losing market share to smaller boutique firms. To understand the potential impact to its market share, the real estate company can review its competitors' commission pricing models and on-line marketing strategies. Information they are looking for is whether the competitors' commission rates are low and aggressive, and how widespread their on-line presence is.
- As part of the component Monitoring Enterprise Risk Management Performance, management may need information on baseline performance as it considers trends in enterprise risk management. It can collect relevant information from attending enterprise risk management conferences and monitoring industry-specific blogs.

Maintaining Information Quality

329. Maintaining the quality of information is essential for enterprise risk management. If the underlying data is inaccurate or incomplete, management may not be able to make sound judgments, estimates, or decisions.
330. High-quality information has the following characteristics:
    - *It is accessible*: The information is easy to obtain in a timely manner by those who need it. Users know what information is available and where it is.
    - *It is accurate*: The information and underlying data are correct.
    - *It is appropriate*: The information is purposeful and sufficient. There is enough information at the right level of detail. Extraneous data is eliminated to avoid inefficiencies, misuse, or misinterpretation.
    - *It is current*: The information is gathered from current sources and at the frequency needed.
    - *It is reliable*: The information is obtained from authorized sources, gathered according to prescribed procedures, and represents events that actually occurred.
    - *It has integrity*: The data and information are protected from manipulation and error.

Example 9.1: Information Quality

331. For a non-profit hospital system, advancements in technology allow physicians to obtain information from devices temporarily attached to their patients. These health-tracking devices provide physicians with minute-by-minute data on pulse, heart rhythm, skin temperature, light exposure, and more. The information gathered has all the characteristics of being high quality: it is accessible, accurate, appropriate, current, reliable, and it has integrity.

332. Information needs to be available to decision-makers in time to be of use. As well, the flow of information must be consistent with the rate of change in the entity's internal and external environments. For example, in areas where hurricanes are common, it is critical for accurate weather forecasts to be updated without delay. A forecast provided several days before an expected hurricane allows residents to prepare for the storm. As the storm approaches, local emergency services require information on weather conditions to assess the potential impacts of the storm. When the hurricane arrives, both residents and emergency services require information in real time to respond appropriately to any emergencies that develop.
333. To ensure high-quality information is available, organizations implement data management systems and establish information management policies with clear lines of responsibility and accountability.

Determining Data Requirements

334. When data is processed, organized, and structured into information about a particular fact or circumstance, it becomes a source for knowledge (e.g., analysis of comments posted on social media to identify potential risks to the entity's reputation). Therefore, data requirements are based on information requirements. For example, a pharmaceutical company's strategy is to expand its market share by developing a new drug targeted to a specific population. To receive approval for its new product, the organization must provide the regulators with information that meets specific compliance requirements such as conclusions regarding the safety of the drug. These conclusions may be based on various data such as demographics of the testing population, number of side effects, duration of studies, and type of application. The organization determines its data requirements based on the need to provide compliance information to an external stakeholder.

335. As with information, data can be collected from a variety of sources and in a variety of forms. Figures 9.1 and 9.2 illustrate internal and external sources of data with examples.

Figure 9.1: Internal Data Sources

Internal Sources	Examples of Internal Data	Qualitative	Quantitative
Board and management meetings	Meeting minutes and notes on potential transactions	✓	
Financial statements and return on investment analyses	Financial inputs for potential investment opportunities		✓
Ethics and behavior-focused training	Employee reactions and responses to ethical scenarios	✓	
Outputs from deals and due diligence	Staffing increases and decreases due to restructuring		✓
Personnel time reports	Hours incurred on time-based projects		✓
Inventory reports	Number of units returned and explanations for return for a core product	✓	✓
Whistle-blower hotline reports	Complaint on supervisor's behavior	✓	✓

Figure 9.2: External Data Sources

External Sources	Examples of External Data	Qualitative	Quantitative
Public indices	Data from water scarcity index for beverage manufacturer or agriculture company considering new locations		✓
Government-produced geopolitical reports and studies	Population changes in emerging markets		✓
Marketing reports from monitoring services	Number of website visits, duration on a page, and conversions into customer purchases		✓
Customer satisfaction survey	Feedback from priority customers about employee interactions	✓	✓

Figure 9.2 continued

External Sources	Examples of External Data	Qualitative	Quantitative
Social media and blogs	Feedback and count of negative and positive comments on a company's new product	✓	✓
Manufacturer reports	Types of products shipped from manufacturer	✓	
Third-party resource reports and publications; industry publications; peer company earnings releases	Market and industry metrics		✓

Managing Data

336. Data must also be well managed in order to meet information requirements and provide the right information to support enterprise risk management. Managing data effectively means preserving and enhancing the quality of the underlying data while addressing consistency, standards, and interoperability throughout its information system and during the full data life cycle. Effective data management considers:

- Governance
- Processes
- Architecture and standards

Data Management Governance

337. The governance of data management helps to deliver standardized, high-quality data to end users in a timely, verifiable, and secure manner. Governance also helps to standardize data architecture, authorize standards, assign accountability, and maintain quality. Effective data governance aligns policies, standards, procedures, organization, and technology. It also defines clear roles and responsibilities for data owners and risk owners.

Data Management Processes

338. Organizational processes and controls embedded in the entity's information system reinforce the reliability of data, or correct it as needed. For example, organizations may use measures to identify instances and patterns of both low- and high-quality data, and the relevance of that data in meeting requirements. Some useful measures include:

- *Data consistency*, which measures the consistency between the data used by analytics and modeling.
- *Data redundancy*, which measures whether data is held in separate places.
- *Data availability*, which measures whether data is available at a required level of performance in varying situations.
- *Data accuracy*, which measures whether data is correct and whether it is retained in a consistent and unambiguous form.
- *Data quality thresholds*, which measures the precision of data used for management decisions.

339. But managing data requires more than using processes and controls to ensure its quality. It also involves preventing issues of quality from occurring in the first place. For example, a retail organization may use automation to help analyze large volumes of sales transactions that occur over a period of time, and it can capture the data it needs through the in-store point-of-sale and on-line systems. The automated system quickly identifies and aggregates sales for specific products that are selling faster or slower than anticipated. Management analyzes the data to make decisions about inventory and product distribution. But it doesn't stop there. The organization also uses automation to gauge the timeliness and precision of the data, answering questions such as: Was the sales data captured during the intended time frame? Is data being delivered in the correct format (e.g., by product code) as required by the inventory and supply chain analysts?

Data Management Architecture and Standards

340. Data management architecture refers to the fundamental design of the business and technology that supports data management. It is composed of models, policies, rules, or standards that dictate which data is collected, and how it is stored, arranged, integrated, and put to use in systems and in the organization. Organizations implement standards and provide rules for structuring information so that the data can be reliably read, sorted, indexed, retrieved, and shared with both internal and external stakeholders, ultimately protecting its long-term value.

Principle 19: Leverages Information Systems

The organization leverages the entity's information systems to support enterprise risk management.

Using Information Systems

341. Information systems provide organizations with the data and information they need to support enterprise risk management. Because the speed at which data is generated, it is often a challenge for management to process and refine it into usable information. Information systems and procedures for collecting, storing, and processing data, and for delivering information, can help entities meet this challenge.

342. Depending on the requirements, information systems may be formal, as with standalone technologies for repeated use, or informal, as with ad hoc web-based surveys (see Example 9.2).

Example 9.2: Information Systems

343. In trying to understand the reasons for high employee turnover, a professional services firm may use information on employee satisfaction. To collect the desired data, the firm sends out an employee survey through the corporate email system and holds periodic firm-wide meetings to solicit direct feedback from employees. These open forums represent an informal component of the firm's information system.

344. In formal systems, an organization can choose the level of efficiency for capturing data. For example, in the case of an entity experiencing an accelerated pace of change and an exponential growth in computing power, the information system may need to be updated so that the data is provided in an automated process. Automation can offer great efficiencies for data aggregation and for maintaining

data quality. In other cases, an organization may be able to collect information manually and directly from an internal or external source. Other organizations may use a combination of manual and automated systems.

Using Enterprise Risk Management Taxonomies

345. An enterprise risk management taxonomy is a comprehensive, common, and stable set of risk categories used across the entity. Many organizations develop risk taxonomies within a particular functional area, such as internal audit, information management, or operational risk management. Enterprise risk management taxonomies can be based on the size, scale, and complexity of the entity with risks organized in sub-categories, which makes using the taxonomy more manageable.

346. Using a taxonomy helps organizations aggregate risk data and information consistently in order to understand the exposures and to identify concentrations of risk. Even more valuable is using a taxonomy to identify risks and consider those that could affect the entity's strategy and business objectives. Taxonomies allow the organization to define specific data attributes, such as risk drivers, risk events, or impacts, and therefore serve as the basis for effective and consistent enterprise risk reporting on the risk profile of the entity.

Sustaining Enterprise Risk Management

347. Organizations can leverage information systems to help sustain enterprise risk management. Information systems can be as simple as spreadsheets and informal discussions or as complex as fully integrated systems and tools. Different systems provide different levels of information on documentation, workflow, assessment and analysis, reporting, visualization, and remediation of risks.

348. Organizations consider the following when selecting or developing supporting technologies:

- *Scope*: How is the technology or tool used to manage risks across the entity (various functions, operating units, geographies, etc.) and at various levels (entity, division, operating unit, function)?
- *Aggregation*: How is the technology or tool used to aggregate risks based on the operating model (organizational structure, legal structure, geographic structure, etc.)?
- *Information quality*: How is the technology or tool used to support the quality of risk information?
- *Consistency and standards*: How is the technology or tool used to help consistently apply and standardize enterprise risk management (e.g., Does the technology require a common taxonomy)?
- *Risk assessment*: How is the technology or tool used to support risk assessment?
- *Reporting*: How is the technology or tool used to support the entity's reporting requirements (e.g., How are graphical risk indicators used to depict risk information and data)?
- *Integration*: How is the technology or tool integrated into existing information systems and other technologies?
- *Cost benefits*: How expensive is the technology or tool in relation to the value and benefits that can be realized?

349. The choice of technology and tools supporting an entity's information system, and the design of that system, can be critical to achieving strategy and business objectives. The decision on what technology to implement depends on many factors, including organizational goals, marketplace needs, competitive requirements, and the associated costs and benefits. An organization uses these factors to balance the benefits of obtaining and managing information and the costs of selecting or developing supporting technologies.

Changing Information System Requirements

350. Management leverages and designs its information systems to meet a broad range of requirements, including those due to internal and external changes. As entities respond to changes in the business context in which they operate, and adapt their strategy and business objectives, they must also review their information systems.

351. For example, an entity that operates in a highly dynamic environment may experience continual changes such as innovative and quick-moving competitors, shifting customer expectations, evolving regulatory requirements, globalization, and technology innovation. In response, management reviews existing information system requirements and adjusts its technology requirements.

352. Continually evolving regulations may require changes to how involved individuals or functions (e.g., legal) interact with and rely on subject matter experts. Shifting customer expectations may require changes to the system to allow for more timely information gathering and more active monitoring of comments on social media. Innovations in technology may present alternatives to change and improve information systems. For example, risk discussions may occur through videoconferences and real-time collaborative tools that replace in-person meetings, and risk information may be electronically shared with a broader audience using cloud services.

Principle 20: Communicates Risk Information

The organization uses communication channels to support enterprise risk management.

Communicating with Stakeholders

353. Various channels are available to the organization for communicating risk data and information to internal and external stakeholders. These channels enable organizations to provide relevant information for use in decision-making.

354. Internally, management communicates the entity's strategy and business objectives clearly throughout the entity so that all personnel at all levels understand their individual roles. Specifically, communication channels enable management to convey:

- The importance, relevance, and value of enterprise risk management.
- The characteristics, desired behaviors, and core values that define the culture of the entity.
- The strategy and business objectives of the entity.
- The risk appetite and acceptable variation in performance.
- The overarching expectations of management and personnel in relation to enterprise risk and performance management.
- The expectations of the organization on any important matters relating to enterprise risk management, including instances of weakness, deterioration, or non-adherence.

355. Management also communicates information about the entity's strategy and business objectives to shareholders and other external parties. Enterprise risk management is a key topic in these communications so that external stakeholders not only understand the performance against strategy but the actions consciously taken to achieve it. External communication may include holding quarterly analyst meetings to discuss performance.

356. An entity with open communication channels can also be on the receiving end of information from external stakeholders. For example, customers and suppliers can provide input on the design or quality of products or services, enabling the organization to address evolving customer demands or preferences. Or inquiries from environmental groups about sustainability approaches could provide an organization with insight into leading approaches or identify potential risks to its reputation. This information may come through email communications, public forums, blogs, and hotlines.

Communicating with the Board

357. Effective communication between the board of directors and management is critical for organizations to achieve the strategy and business objectives and to seize opportunities within the business environment. Communicating about risk starts by defining risk responsibilities clearly: who needs to know what and when they need to act. Organizations should examine their risk governance structure to ensure that responsibilities are clearly allocated and defined at the board and management levels and that the structure supports the desired risk dialogue. The board's responsibility is to provide oversight and ensure the appropriate measures are in place so that management can identify, assess, prioritize, and respond to risk (see Example 9.3).

Example 9.3: Communicating with the Board

358. A global car manufacturer aiming to improve risk communication chose to revise its risk governance structure by elevating its chief risk officer position to ensure risk was integrated into all discussions of business strategy. Risk issues are now discussed by the full board. The company found that bringing risk out of a board committee and embedding enterprise risk management responsibilities into the management team better integrated risk and strategy discussions and increased clarity about risk.

359. To communicate effectively, the board of directors and management must have a shared understanding of risk and its relationship to strategy and business objectives. In addition, directors need to develop a deep understanding of the business, value drivers, and strategy and associated risks. Many board members use on-site visits as a communication channel to engage with management and personnel to understand operations and management.

360. Board and management continually discuss risk appetite. As part of its oversight role, the board ensures that communications regarding risk appetite remain open. It may do this by holding formal quarterly board meetings, and by calling extraordinary meetings to address specific events, such as cyber terrorism, CEO succession, or mergers. The board and management can use the risk appetite statement as a touchstone, allowing them to identify those risks that are on or off strategy, monitor the entity's risk profile, and track the effectiveness of enterprise risk management programs. Given the strong link to strategy, the risk appetite statement should be reviewed as strategy and business objectives evolve.

361. Management provides any information that helps the board fulfill its oversight responsibilities concerning risk. There is no single correct method for communicating with the board, but the following list offers some common approaches:

- Address risks as determined by the entity's strategy and business objectives.
- Capture and align information at a level that is consistent with directors' risk oversight responsibilities and with the level of information determined necessary by the board.
- Ensure reports present the entity's risk profile as aligned with its risk appetite statement, and link reported risk information to policies for exposure and tolerances.
- Provide a longitudinal perspective of risk exposures including historical data, explanations of trends, and forward-looking trends explained in relation to current positions.

- Update at a frequency consistent with the pace of risk evolution and severity of risk.
- Use standardized templates to support consistent presentation and structure of risk information over time.

362. Management should not underplay the importance of qualitative open communications with the board. A dynamic and constructive risk dialogue must exist between management and the board, including a willingness to challenge any assumptions underlying the strategy and business objectives. Boards can foster an environment in which management feels comfortable bringing risk information to the board even if they do not yet have a clearly defined enterprise risk management plan. Management may be uncomfortable discussing emerging risks with the board at a time when the severity of these risks is often unclear. By being open to conversations where there is not yet a final resolution, the board can encourage these conversations with management to provide more timely and insightful dialogue, rather than waiting for these risks to evolve within the entity.

Methods of Communicating

363. For information to be received as intended, it must be communicated clearly. To be sure communication methods are working, organizations should periodically evaluate them. This can be done through existing processes such as employee performance evaluations, annual management reviews, and other feedback programs.

364. Methods vary widely, from holding face-to-face meetings, to posting messages on the entity`s intranet, to announcing a new product at an industry convention, to broadcasting to shareholders globally through social media and newswires.

365. Communication methods can take the form of:

- *Electronic messages* (e.g., emails, social media, text messages, instant messaging).
- *External/third-party materials* (e.g., industry, trade, and professional journals, media reports, peer company websites, key internal and external indices).
- *Informal/verbal* (e.g., one-on-one discussions, meetings).
- *Public events* (e.g., roadshows, town hall meetings, industry/technical conferences).
- *Training and seminars* (e.g., live or on-line training, webcast and other video forms, workshops).
- *Written internal documents* (e.g., briefing documents, dashboards, performance evaluations, presentations, questionnaires and surveys, policies and procedures, FAQs).

366. In addition to the channels discussed above, separate lines of communication are needed when normal channels are inoperative or insufficient for communicating matters requiring heightened attention. Many organizations provide a means to communicate anonymously to the board of directors or a board delegate—such as a whistle-blower hotline. Many organizations also establish escalation protocols and policies to facilitate communication when there are exceptions in standards of conduct or inappropriate behaviors occurring.

Principle 21: Reports on Risk, Culture, and Performance

The organization reports on risk, culture, and performance at multiple levels of and across the entity.

Identifying Report Users and Their Roles

367. Reporting supports personnel at all levels to understand the relationships between risk, culture, and performance and to improve decision-making in strategy- and objective-setting, governance, and day-to-day operations. Reporting requirements depend on the needs of the report user. Report users may include:

- Management and the board of directors with responsibility for governance and oversight of the entity.
- Risk owners accountable for the effective management of identified risks.
- Assurance providers who seek insight into performance of the entity and effectiveness of risk responses (e.g., a CPA firm).
- External stakeholders (regulators, rating agencies, community groups, and others).
- Other parties that require reporting of risk in order to fulfill their roles and responsibilities.

368. It is also important to understand the governance and operating models of respective report users. Each report user will require different levels of detail of risk and performance information in order to fulfill their responsibilities in the entity. Reporting must also make clear the interrelationships between users, and the related effect across the entity.

369. Risk information presented at different levels cascades down into the entity and flows up to support higher levels of reporting. For example, reports to the board support decisions on risk appetite and company strategy. Reports from senior management present a more granular level and support decisions on strategic planning and budgeting, as well as decisions at the divisional and/or functional level. The next layer of reporting is even more granular and supports divisional and functional leaders in planning, budgeting, and day-to-day operations. This level of reporting should align with senior management reporting and board reporting. At higher levels, risk reporting encapsulates the portfolio view.

370. Risk reporting may be done by any team within the operating model. Teams prepare reports, disclosing information in accordance with their risk management responsibilities. For example, teams will prepare risk information as part of financial and budgeting planning submissions to support requests for additional resources to maintain or prevent the risk profile from deteriorating.

Reporting Attributes

371. Reporting combines quantitative and qualitative risk information, and the presentation can range from being fairly simple to more complex depending on the size, scope, scale, and complexity of the entity. Risk information supports management in decision-making, although management must still exercise business judgment in the pursuit of business objectives.

372. In reporting, history can relay meaningful, useful information, but an emphasis on being forward-looking is of more benefit. Knowing the end-to-end processes taken to fulfill an entity's mission and vision, as well as the business environment in which entity operates, can help management make a connection between historical information and potential early-warning information. Early-warning analytics of key trends, emerging risks, and shifts in performance may require both internal and external information.

Types of Reporting

373. Risk reporting may include any or all of the following:

- *Portfolio view of risk* outlines the severity of the risks at the entity level that may impact the achievement of strategy and business objectives. The reporting of the portfolio view highlights the greatest threats to the entity, interdependencies between specific risks, and opportunities. The portfolio view of risk is typically found in management and board reporting.
- *Profile view of risk*, similar to the portfolio view, outlines the severity of risks, but focuses on different levels within the entity. For example, the risk profile of a division or operating unit may feature in designated risk reporting for management or those areas of the entity.
- *Analysis of root causes* enables users to understand assumptions and changes underpinning the portfolio and profile views of risk.
- *Sensitivity analysis* measures the sensitivity of changes in key assumptions embedded in strategy and the potential impact on strategy and business objectives.
- *Analysis of new, emerging, and changing risks* provides the forward-looking view to anticipate changes to the risk universe, effects on resource requirements and allocation, and the anticipated performance of the entity.
- *Key performance indicators and measures* outline the acceptable variation in performance of the entity and potential risk to a strategy or business objective.
- *Trend analysis* demonstrates movements and changes in the portfolio view of risk, risk profile, and performance of the entity.
- *Disclosure of incidents, breaches, and losses* provides insight into effectiveness of risk responses.
- *Tracking enterprise risk management plans and initiatives* provides a summary of the plan and initiatives in establishing or maintaining enterprise risk management practices. Investment in resources, and the urgency by which initiatives are completed, may also reflect the commitment to enterprise risk management and culture by organizational leaders in responding to risks.

374. Risk reporting is supplemented by commentary and analysis by subject matter experts. For example, compliance, legal, and technology experts often provide commentary and analysis on the severity of risk, effectiveness of risk responses, drivers for changes in trend analysis, and industry developments and opportunities the entity may have.

Reporting Risk to the Board

375. At the board level, there is likely to be both formal reporting and informal information sharing. For example, the board may have informal discussions about the possibility of strategy and implications of alternative strategies while using risk profiles and other analyses to support the discussions. Formal reporting plays a more integral role when the board exercises other responsibilities including considering the risks to executing strategy, reviewing risk appetite, or overseeing enterprise risk management practices deployed by management.

376. There are a number of ways management may report to a board, but it is critical that the focus of reporting be the link between strategy, business objectives, risk, and performance. Reporting to the board is the highest level of reporting and will include the portfolio view. Reporting to the board should foster discussions of the performance of the entity in meeting its strategy and business objectives and the risk and impact of potential risk in meeting those objectives.

Reporting on Risk Culture

377. An entity's culture is grounded in behavior and attitudes, and measuring it is often a very complex task. Reporting on culture may be embodied in:

- Analytics of cultural trends.
- Benchmarking to other entities or standards.
- Compensation schemes and the potential influence on decision-making.
- "Lessons learned" analyses.
- Reviews of behavioural trends.
- Surveys of risk attitudes and risk awareness.

Key Indicators

378. Key risk indicators are used to predict a risk manifesting. They are usually quantitative, but can be qualitative. Key risk indicators are reported to the levels of the entity that are in the best position to manage the onset of a risk where necessary. They should be reported in tandem with key performance indicators to demonstrate the interrelationship between risk and performance. Key risk indicators support a proactive approach to performance management (see Example 9.4).

Example 9.4: Using Key Risk Indicators

379. A government agency wants to retain competent individuals. The business objective that supports retaining competent individuals has as a target maintaining turnover rates at less than 5% per year. A key risk indicator would be a percentage of personnel eligible to retire within five years. Anything higher than 5% indicates that risk to the target is potentially manifesting. A key performance indicator is the actual turnover rate. Key performance indicators are based on historical performance, and while understanding historical performance can establish baselines, the rate trending upwards would not necessarily identify a risk manifesting.

380. Key risk indicators and key performance indicators can be reflected in a single measure. For example, in a manufacturing company, production volumes and the thresholds around them can be viewed through a risk lens. Production volumes above the target can be seen as potential risks to quality, and production volumes below the target can suggest potential risk around the infrastructure that supports the process.

381. Key risk indicators are reported along with corresponding targets and acceptable variations. Where an entity lies on the risk culture spectrum, whether risk averse or risk aggressive, will help determine the key risk indicators and key performance indicators that are tracked as well as the acceptable variation in performance.

Reporting Frequency and Quality

382. Management works closely with those who will use reports to identify what information is required, how often they need the reports, and their preferences in how reports are presented. Management is responsible for implementing appropriate controls so that reporting is accurate, clear, and complete.

383. The frequency of reporting should be commensurate with the severity and priority of the risk. Reporting should enable management to determine the types and amount of risk assumed by the organization, its ongoing appropriateness, and the effectiveness of existing risk responses. For example, changes in stock prices, or competitor pricing in the hospitality or airline industries, may be reported on daily, commensurate with the potential changes in risk. In contrast, reporting on the risks emanating from an organization's progress toward long-term strategic projects and initiatives may be monthly or quarterly.

10. Monitoring Enterprise Risk Management Performance

Chapter Summary

384. Monitoring enterprise risk management performance considers how well the enterprise risk management components are functioning over time and in light of substantial changes.

Principles Relating to Monitoring Entity Performance

22. **Monitoring Substantial Change**—The organization identifies and assesses internal and external changes that may substantially impact strategy and business objectives.
23. **Monitors Enterprise Risk Management**—The organization monitors enterprise risk management performance.

Introduction

385. Monitoring provides insight into how well the organization has implemented enterprise risk management within the entity. The business objectives and the components of enterprise risk management may change over time as the entity adapts to shifting internal and external environments. In addition, current practices and processes may no longer apply, or may be deemed insufficient to support the achievement of new or updated business objectives.

Principle 22: Monitoring Substantial Change

The organization identifies and assesses internal and external changes that may substantially impact strategy and business objectives.

Integrating Monitoring into Business Processes

386. Monitoring substantial change, which may lead to new or changed risks, should be built into business processes and performed continually. Many management practices can identify substantial changes in the ordinary course of running the business. For example, reviewing the plan for integrating a newly acquired joint business venture may identify the need for future enhancements of information technology.

387. Substantial changes such as acquiring an entity or implementing a new system could potentially change the entity's portfolio view of risk or impact how enterprise risk management functions. In the case of an acquisition, integrating the acquired company's operations could impact the existing culture and risk ownership. Implementing a new system could present new exposures related to information security, which could influence how data is captured and managed.

388. Organizations consider how change can affect enterprise risk management and the achievement of strategy and business objectives. This requires identifying internal and external environmental changes related to the business context as well as changes in culture. Some examples of substantial change are highlighted below.

Internal Environment

- *Rapid growth*: When operations expand quickly, existing structures, business processes, information systems, or resources may be affected. Information systems may not be able to effectively meet risk information requirements because of the increased volume of transactions. Risk oversight roles and responsibilities may need to be redefined in light of organizational and geographical changes due to an acquisition. Resources may be strained to the point where existing risk responses and actions break down. For instance, supervisors may not successfully adapt to higher activity levels that require adding manufacturing shifts or increasing personnel.
- *New technology*: Whenever new technology is introduced, risk responses and management actions will likely need to be modified. For instance, introducing sales capabilities through mobile devices may require access controls specific to that technology. Training may be needed for users. New technology may also enhance enterprise risk

management. For example, a new system of using mobile devices that captures previously unavailable sales information gives management the ability to monitor performance, forecast potential sales, and make real-time inventory decisions.

- *Substantial changes in leadership and personnel*: A change in management may affect enterprise risk management. A newcomer to management may not understand the entity's culture and have a different philosophy, or may focus solely on performance to the exclusion of risk appetite or acceptable variation in performance (see Example 10.1).

Example 10.1: Substantial Changes in Leadership and Personnel

389. The new chief executive officer of a global technology company that focuses on revenue growth and aggressive cost reduction sends a message that a prior focus on operating within the entity's risk appetite is now less important. She reduces staffing levels by 15% in an attempt to decrease costs, thereby affecting the ability to manage production and impeding the ability to operate within the target residual risk. The reduced personnel level also presents a risk to the entity's ability to meet minimum production requirements and operate within acceptable variation in performance.

External Environment

- *Changing regulatory or economic environment* can result in increased competitive pressures, changes in operating requirements, and different risks. If a large-scale failure in operations, reporting, and compliance occurs in one entity, regulators may introduce broad regulations that affect all entities within an industry. For instance, if toxic material is released in a populated or environmentally sensitive area, new industry-wide transportation restrictions may be introduced that affect an entity's shipping logistics. If a publicly traded company is seen to have poor transparency, enhanced regulatory reporting requirements may be introduced for all publicly traded companies. The revelation of patients being treated poorly in a care facility may prompt additional care requirements for all care facilities. And a more competitive environment may drive individuals to make decisions that are not aligned with the entity's risk appetite and increase the risk exposures to the entity. Each of these changes may require an organization to closely examine the design and application of its enterprise risk management.

Culture

- *Mergers and acquisitions* can result in changes to the culture that may affect enterprise risk management. As noted above, new leadership may have a different attitude and philosophy about enterprise risk management. Additionally, an acquisition could alter an entity's mission and vision and affect decision-making (see Example 10.2).

Example 10.2: How Mergers and Acquisitions Can Affect Culture

390. A large investment bank has acquired a commercial bank to expand its portfolio and diversify its service offerings. Prior to the acquisition, the investment bank's overarching risk appetite was high and the bank was viewed as a risk aggressor on the spectrum of risk. The bank previously focused on maximizing the wealth of its large corporate customers. After the acquisition, the bank altered its mission and vision to include a focus on preserving the wealth of its new customers, individuals, and small businesses. The bank recognized the importance of establishing long-lasting relationships with its new customers and understood their lower capacities for risk. After considering its new mission and vision, and with input from its new stakeholders, the bank adjusted its overarching risk appetite. The new risk appetite cascades throughout the entity, influencing the bank's overall culture, decision-making, and behaviors. The bank is now externally viewed as a risk-averse entity.

- *Restructuring* can change a company's culture, affecting enterprise risk management. For example, a consumer products company currently operates in a decentralized manner with the business divisions in various locations. Management decides to centralize operations and relocate all the divisions to one location. As a result, some employees must relocate, and some jobs are eliminated to avoid duplication. Management's decision will affect the overall culture through instability, which may affect overall employee productivity and job satisfaction. In response, management should re-evaluate its strategy and business objectives during the planning for restructuring.

391. Identifying substantial changes, evaluating their impact, and responding to the changes are iterative processes that can affect several components of enterprise risk management. It can be useful to conduct a "post-mortem" after a risk event to review how well the organization responded and to consider what lessons learned could be applied to future events.

Principle 23: Monitors Enterprise Risk Management

The organization monitors enterprise risk management performance.

Pursuing Improvement

392. Even those entities with suitable enterprise risk management can become more efficient. By embedding continual evaluations into an integrated enterprise risk management system, organizations can systematically identify potential improvements. Separate evaluations may also be helpful.

393. Pursuing improved enterprise risk management should occur throughout the entity, with management assessing what component may be improved (see Example 10.3).

Example 10.3: Continual Improvement

394. A government agency's enterprise risk management is performing very well in the Risk Governance and Culture component, but not as well in the Information and Communications component. While management monitors improvement opportunities for all enterprise risk management components, it concentrates its continual evaluations on Information and Communications.

395. Management pursues continual improvement throughout the entity (functions, operating units, divisions, and entity level) to improve the efficiency and usefulness of enterprise risk management at all levels. Opportunities to revisit and improve efficiency and usefulness may occur in any of the following areas:

- *New technology*: New technology may offer an opportunity to improve efficiency. For example, an entity that uses customer satisfaction data finds it voluminous to process. To improve efficiency it implements a new data-mining technology that pinpoints key data points quickly and accurately.
- *Historical shortcomings*: Monitoring can identify historical shortcomings or the causes of past failures, and that information can be used to improve enterprise risk management. For example, management in an entity observes that there have been shortcomings noted over time related to risk assessment. Although management compensates for these, the organization decides to improve its risk assessment process to reduce the number of shortcomings and enhance enterprise risk management.

- *Organizational change*: By pursing continual improvement, an organization can identify the need for organizational changes such as a change in the governance model. For example, an enterprise risk management function reports to the chief financial officer, but when the entity redevelops its strategy group, it decides to realign the responsibility for enterprise risk management to that reorganized group.
- *Risk appetite*: Monitoring provides clarity on factors that affect the entity's risk appetite. It also gives management an opportunity to refine its risk appetite. For example, management may monitor the performance of a new product over a year and assess the volatility of the market. If management determines that the market is peforming well and is less volatile than originally thought, the organization can respond by increasing its risk appetite for similar future initiatives.
- *Risk taxonomy*: An organization that continually pursues improvement can identify patterns as the business changes, which can lead the entity to revise its risk taxonomy. For example, one entity's risk taxonomy does not include cyber risk, but now that the entity has decided to offer several on-line products and services, it is revising the taxonomy to include cyber risk so it can accurately map its strategy.
- *Communications*: Monitoring can identify outdated or poorly functioning communication processes. For example, in monitoring performance an organization discovers that emails are not successfully communicating its initiatives. In response, the organization decides to highlight initiatives through a blog and instant message feed to appeal to its changing workforce.
- *Peer comparison*: Monitoring industry peers can help an organization determine if it is operating outside of industry performance boundaries. For example, a global package delivery provider discovered during a peer review that its operations in Asia were performing significantly below its major competitor. Consequently, it is planning to review and, if necessary, revise its strategy to increase its competitiveness and, hence, its performance in Asia.
- *Rate of change*: Management considers the rate that the business context evolves or changes. For example, an entity in an industry where technology is quickly changing or where organizational change happens often may have more frequent opportunities to improve the efficiency and usefulness of enterprise risk management, but an entity operating in an industry with a slower rate of change in technology will likely have fewer opportunities.

Using Baseline Information

396. Understanding the current and desired future state of enterprise risk management provides useful baseline information for improving its efficiency and usefulness. When assessing opportunities to improve, it is necessary to understand how management has designed and implemented enterprise risk management within each of the five components. It is also important to understand the entity's desired future state within each of the five components so potential improvements for efficiency and usefulness can be identified and continual improvement can occur.
397. Enterprise risk management varies among entities. Consequently, opportunities must be tailored to accommodate each entity. If an entity does not have a baseline understanding of enterprise risk management, it may need to increase monitoring. Also, when change occurs within any of the five components, the baseline may need to be evaluated or updated to better assess future opportunities.

Appendices

A. Glossary of Terms

Acceptable Variation in Performance: The boundaries of acceptable outcomes related to achieving business objectives.

Business Context: The trends, events, relationships and other factors that may influence, clarify, or change an entity's current and future strategy and business objectives.

Business Objectives: Those measurable steps the organization takes to achieve its strategy.

Compliance Objectives: Those objectives that relate to an organization conforming with laws and regulations applicable to an entity.

Components: In the context of this publication, the five enterprise risk management components: (1) Risk Governance and Culture; (2) Risk, Strategy, and Objective-Setting; (3) Risk in Execution; (4) Risk Information, Communication, and Reporting; and (5) Monitoring Enterprise Risk Management Performance.

Core Values: The entity's beliefs and ideals about what is good or bad, acceptable or unacceptable, which influence the behavior of the organization.

Culture: The attitudes, behaviors, and understanding about risk, both positive and negative, that influence the decisions of management and personnel and reflect the mission, vision, and core values of the organization.

Data: Raw facts that can be collected together to be analyzed, used, or referenced.

Entity: Any form of for-profit, not-for-profit, or governmental body. An entity may be publicly listed, privately owned, owned through a cooperative structure, or any other legal model.

Enterprise Risk Management: The culture, capabilities, and practices, integrated with strategy-setting and its execution, that organizations rely on to manage risk in creating, preserving, and realizing value.

External Environment: Anything outside of the organization that influences the entity's ability to achieve its strategy and business objectives.

External Stakeholders: Any parties not directly engaged in the entity's operations but who are impacted by the entity, directly influence the entity's business environment, or influence the entity's reputation, brand, and trust.

Event: An occurrence or set of occurrences.

Framework: The five components consisting of (1) Risk Governance and Culture; (2) Risk, Strategy, and Objective-Setting; (3) Risk in Execution; (4) Risk Information, Communication, and Reporting; and (5) Monitoring Enterprise Risk Management Performance.

Impact: The result or effect of a risk. There may be a range of possible impacts associated with a risk. The impact of a risk may be positive or negative relative to the entity's strategy or business objectives.

Information: Processed, organized, and structured data concerning a particular fact or circumstance.

Inherent Risk: The risk to an entity in the absence of any explicit or targeted actions that management might take to alter the risk's severity.

Internal Control: A process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance. (For more discussion, see *Internal Control—Integrated Framework*.)

Internal Environment: The environment within the entity that will affect the achievement of its strategy and business objectives.

Internal Stakeholders: Parties working within the entity such as employees, management, and the board.

Likelihood: The possibility that a given event will occur.

Mission: The entity's core purpose, which establishes what it wants to accomplish and why it exists.

Operations Objectives: Those objectives that are related to the effectiveness and efficiency of an entity's operations, including performance and profitability targets, and safeguarding resources.

Opportunity: An action or potential action that creates or alters goals or approaches for creating, preserving, and realizing value.

Organization: The term used to describe, collectively, the board of directors, management, and other personnel of an entity.

Organizational Sustainability: The ability of an entity to withstand the impact of large-scale events.

Performance Management: All efforts to achieve or exceed the strategy and business objectives.

Portfolio View: A composite view of risk the entity faces, which positions management and the board to consider the types, severity, and interdependencies of risks and how they may affect the entity's performance relative to its strategy and business objectives.

Practices: The methods and approaches deployed within an entity relating to manage the risk.

Reasonable Expectation: An organization's agreed-upon level of uncertainty that it determines is appropriate for that entity (recognizing that no one can predict risk with precision).

Reporting Objectives: Those objectives that relate to reporting on financial and non-financial performance, both internally and externally.

Residual Risk: The risk remaining after management has taken explicit or targeted action to alter the risk's severity.

Risk: The possibility that events will occur and affect the achievement of strategy and business objectives.

Risk Appetite: The types and amount of risk, on a broad level, an organization is willing to accept in pursuit of value.

Risk Capacity: The maximum amount of risk that an entity is able to absorb in the pursuit of strategy and business objectives.

Risk Profile: A composite view of the risk assumed at a particular level of the entity, or aspect of the business model that positions management to consider the types, severity, and interdependencies of risks, and how they may affect performance relative to its strategy and business objectives.

Risk Universe: All risks that could affect an entity.

Severity: A measurement of considerations such as the likelihood and impact of events or the time it takes to recover from events.

Stakeholders: Parties that have a genuine or vested interest in the entity.

Strategy: The organization's plan to achieve its mission and vision and apply its core values.

Uncertainty: The state of not knowing how potential events may or may not manifest.

Vision: The entity's aspirations for its future state or what the organization aims to achieve over time.

B. Roles and Responsibilities

398. 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.

399. 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 the context of a "lines of accountability model" to achieve the entity's strategy and business objectives.

400. 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 to 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. These factors within an organization's business context may tend to establish roles across any number of different lines of accountability with specific regulatory guidance and oversight. Some organizations may refer to the board of directors as a line of accountability based on its specific roles, responsibilities, and accountabilities for that entity. Regardless of the number of lines of accountability, however, the roles, responsibilities, and accountabilities are defined to allow for clear "ownership" of strategy and risk that fits within the governance structure, reporting lines, and culture of the entity.

Board of Directors and Dedicated Committees

401. 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 6 through 10), these governance structures are commonly referred to as "the board of directors" (even if in a specific entity they are named something different).

402. The board of directors is responsible for providing risk oversight of enterprise risk management. 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 the time necessary to fulfill their day-to-day risk oversight responsibilities and accountabilities. Figure B.1 lists typical board oversight practices of enterprise risk management.

Figure B.1: Board Oversight Practices

Enterprise Risk Management Component	Risk Oversight Practices
Risk 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
Risk, 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
Risk in Execution	• Reviews the entity's strategy and underlying assumptions against the portfolio view of risk • Sets expectations for the 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 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

Figure B.1 continued

Enterprise Risk Management Component	Risk Oversight Practices
Risk Information, Communication, and Reporting	• Establishes the information, underlying data, and formats (graphs, charts, risk curves, and other visuals) 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
Monitoring Enterprise Risk Management Performance	• 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

403. 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 clear focus on individual areas of risk. Where a particular committee has not been established for a specific risk area, the oversight responsibilities are carried out by the board itself.

404. 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 risks 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 to motivate without providing incentives for undue risk taking. It also oversees that management balances 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 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 orientations and training and evaluates oversight processes and structures (e.g., board/committee evaluations).

Management and the Three Lines of Accountability

405. 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

406. The chief executive officer (CEO) is accountable to the board of directors and is responsible for designing, implementing, and executing enterprise risk management to enable the achievement of 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.

407. 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 and 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

408. One of the more prominent roles in enterprise risk management is that of the chief risk officer. This position, which generally reports directly to the chief executive officer, is tasked with overseeing enterprise risk management as a second line of accountability. 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.

409. 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 chief executive officer. 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 chief risk officer. These entities often align staff within divisions, operating units, and functions with the chief risk officer to support enterprise risk management efforts across the entity.

410. The chief risk officer 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.
- 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 chief executive officer 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

411. 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. Examples of management for a larger public or private entity, a smaller business entity, and a government entity are noted in Figure B.2.

Figure B.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 strategy officer	• President • Chief financial officer/vice president (VP) of finance/ finance director/head of finance/controller • Director of risk management/ head of risk management • Chief operating officer • General manager/VP of operations • VP marketing/marketing manager • VP human resources/human resources director • VP of technology/IT manager	• Secretary • Assistant secretary/deputy director/undersecretary • Chief financial officer • Chief information officer • Chief of human resources • Chief of staff • Deputy assistant secretary/ directorate • General counsel • Inspector general

412. 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.
- 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.
- Communicating the enterprise risk management process to the CEO and the board.

413. 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 consistently applied.

414. 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 execute the enterprise risk management process that 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

415. Management is responsible for identifying and managing the performance and risks resulting from practices and systems for which they are accountable. The first line is also responsible for the risks inherent to the strategy and business objectives. As the principal owners of risk, they set business objectives, establish acceptable variation in performance, train personnel and reinforce risk responses. In short, the first line implements and executes the day-to-day tasks to manage performance and risks taken to achieve strategy and business objectives.

Second Line: Support Functions

416. 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 lines 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.

417. 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.

418. 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.

Third Line: Assurance Functions

419. 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

420. 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.

421. In an external audit, the auditor expresses an opinion on the fairness of the financial statements in conformity with generally accepted accounting principles, 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 control that come to the auditor's attention, and recommendations for improvement.

422. 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 in each of these areas. The information is reported to management and, depending on its significance, to the board of directors or audit committee.

423. 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.

C. Risk Profile Illustrations

Introduction to Risk Profiles

424. A risk profile provides the composite view of risks related to a specific strategy or business objective. Risk profiles are used to help organizations evaluate alternative strategies and support the process of identifying and assessing risks.

425. 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 representation illustrates 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.

426. This appendix offers examples of how risk profiles may be developed and applied to support the organization in applying the principles of the Framework (Chapters 6 through 10).

Developing Risk Profiles

427. 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.

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

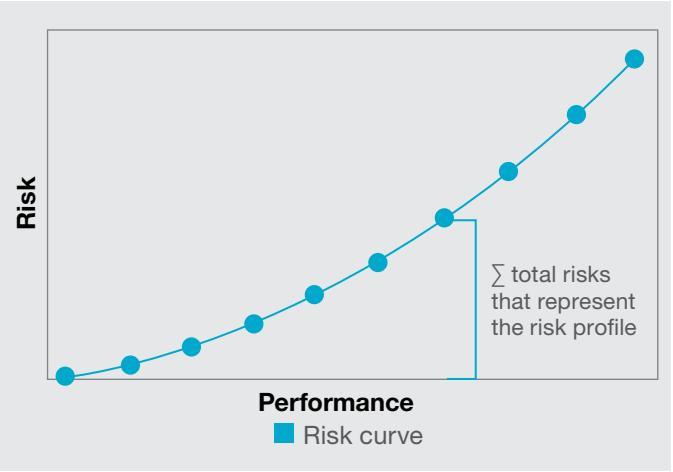
- The relationship between risk and performance, noting that the amount of risk for a given strategy or business objective is typically not static and will change for differing levels of performance.
- Assumptions underlying the risk assessment for a given strategy or business objective.
- The level 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.

429. 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 C.1). The resulting line is often referred to as a "risk curve" or "risk profile."

430. 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.

431. 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 more quantitative approach, such as probabilistic modeling, regression analysis, or other techniques. 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, and benchmarking. Example C.1 illustrates how one entity plotted its risk profile.

Figure C.1: Risk Profile



Example C.1: Developing Risk Profile

432. 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 with respect to this business objective:

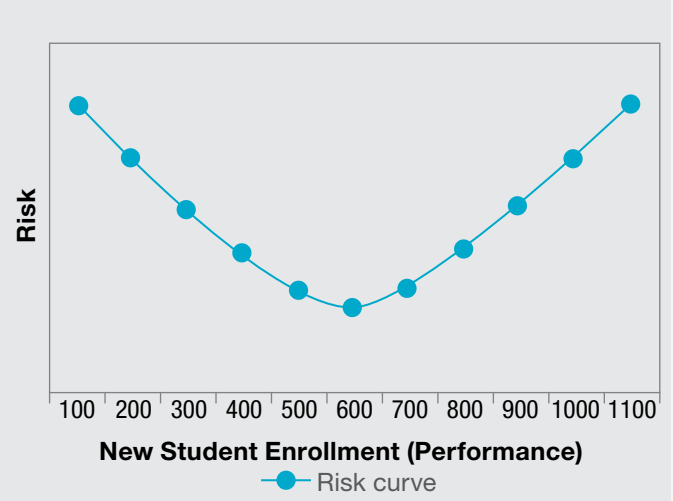
- Failing to build sufficient interest and awareness of the courses to generate growth in student applications, which could impact the university's reputation.
- Generating actual or perceived conflict of interest between academic freedom and the new curriculum.
- Failing to attract and retain additional 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.

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

434. 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 (Figure C.2). 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.

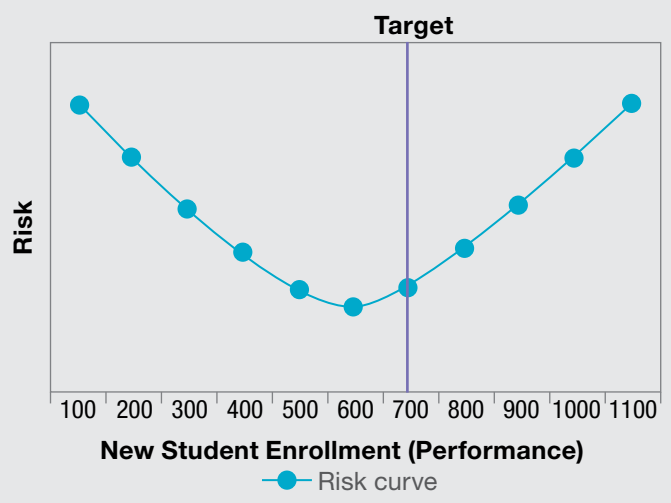
Figure C.2: Risk Profile—Introducing a New Curriculum



Example C.1 continued

- 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?

Figure C.3: Risk Profile—Introducing a New Curriculum



435. 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. Figure C.3 illustrates the resulting risk profile:

- There is a high amount of risk assumed if only 100 new students enroll as a result 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 represents an incremental increase in risk. The university has established that it can accept a maximum of 1,100 new students.

436. 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. Figure C.3 illustrates this target and the amount of risk the university is willing to assume in the pursuit of the objective.

Risk, Strategy, and Objective-Setting

Incorporating Risk Appetite

437. Using a risk profile, the organization can outline its risk appetite in relation to a proposed strategy or business objective. In Figure C.4, 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.

438. 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.

439. Organizations may want to also incorporate an additional parallel line above risk appetite to indicate risk capacity, shown in Figure C.5.

Figure C.4: Risk Profile with Risk Appetite

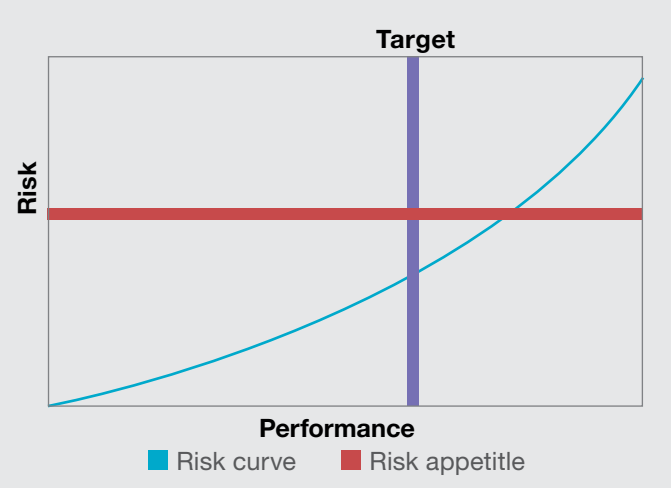
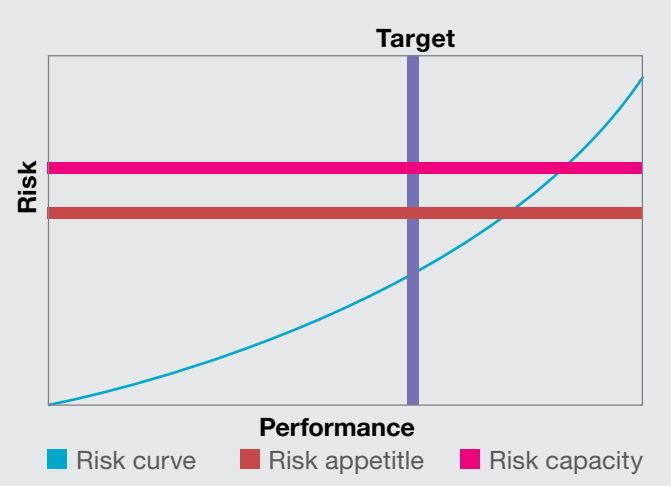


Figure C.5: Risk Profile with Risk Capacity

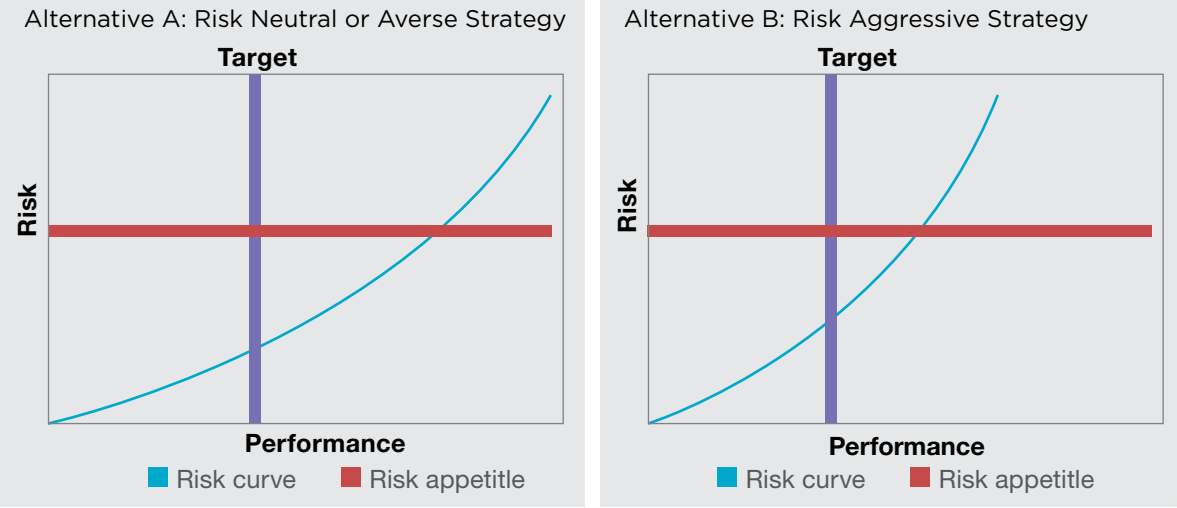


Using Risk Profiles to Consider Alternative Strategies

440. Organizations can use graphical illustrations to 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.

441. Figure C.6 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.

Figure C.6: Risk Profile of Alternative Strategies



442. Conversely, risk-taking entities such as startups 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.

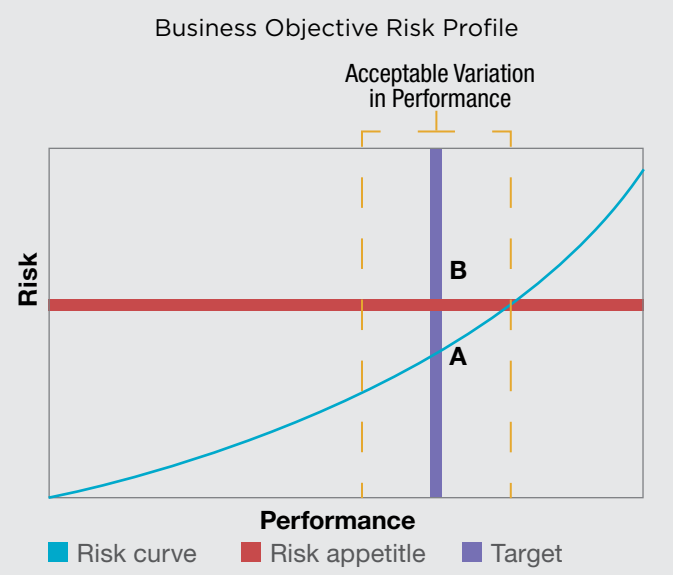
443. Quantitative and qualitative techniques are used to develop the profile of potential risks and may be the same tools that are then used to support risk identification and assessment processes. This includes quantitative analysis and modeling where there is sufficient data. Where data is not available,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

Considering Risk in Establishing Business Objectives and Setting Performance Targets

444. 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.

445. 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 C.7). 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 C.7: Risk Profile with Performance Targets



Demonstrating Acceptable Variation in Performance Using Risk Profiles

446. Having set the target, the organization 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 Execution

447. 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.

448. 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 determine it needs to update the list of expected risks due to changes in the business context having occurred.

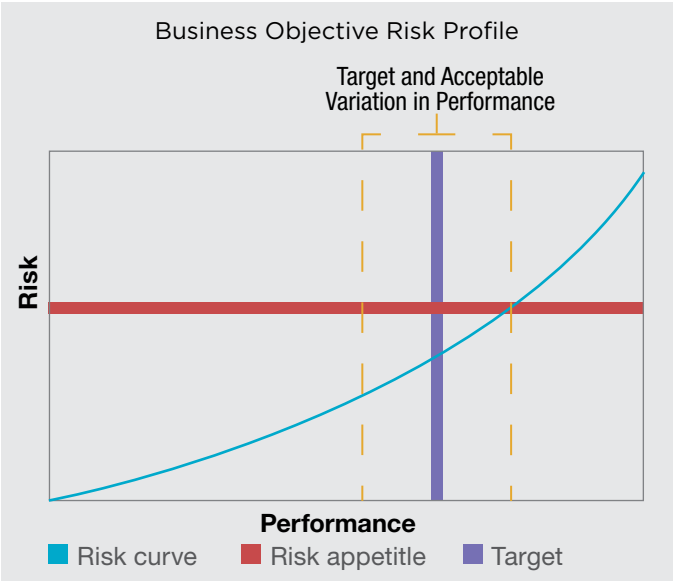
449. The outputs of the risk identification process, the risk universe, form the basis from which an organization is able to construct a more reliable risk profile.

Using Risk Profiles when Assessing Risk

450. 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.

Figure C.8: Assessing Risk using a Risk Profile



451. The risk profile in Figure C.8 depicts the amount of risk within an assumed time horizon. In order to incorporate time into the risk profile, management must define the performance target with reference to a time period.

452. 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 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.

453. 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.

454. 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, a reputable technology company is analyzing whether to launch 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.

455. 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, the same technology company is assessing the risk of maintaining operations in a foreign country based on a volatile exchange rate. In plotting the curve, the company may employ modeling to identify sufficient points outlining the severity of its foreign exchange exposure.

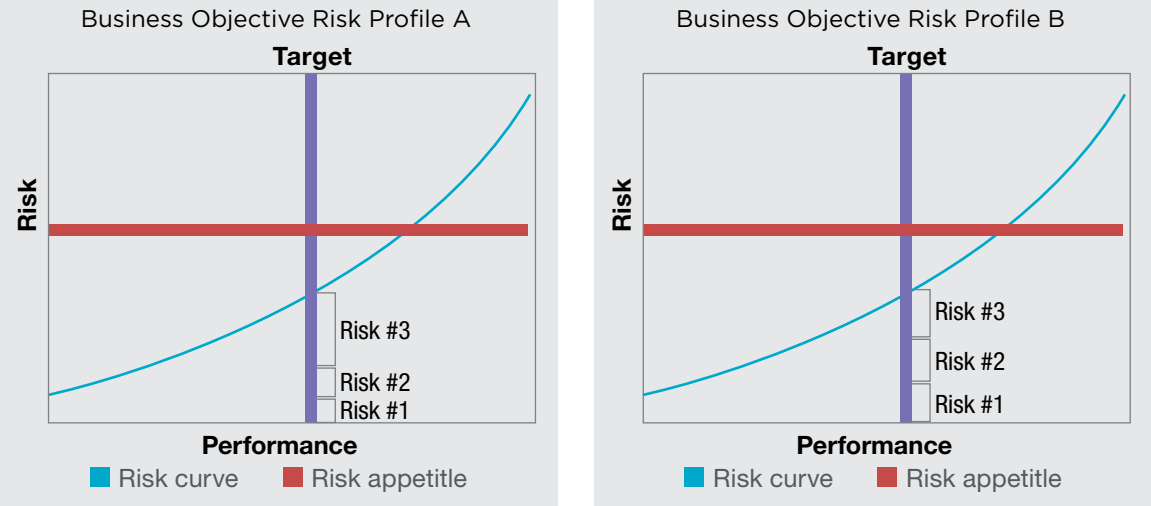
Using Risk Profiles when Prioritizing Risks

456. 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.

457. Many organizations choose to use severity as a prioritization criterion. For example, consider the risk profiles in Figure C.9. 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 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 C.9: Using Risk Profiles to Compare Risks Impacting Business Objectives



Using Risk Profiles when Considering Risk Responses

458. 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 in appetite. Alternatively, for risks that are already in 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.
- *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 many 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.

459. Figure C.10 shows how a risk profile changed after executing 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.

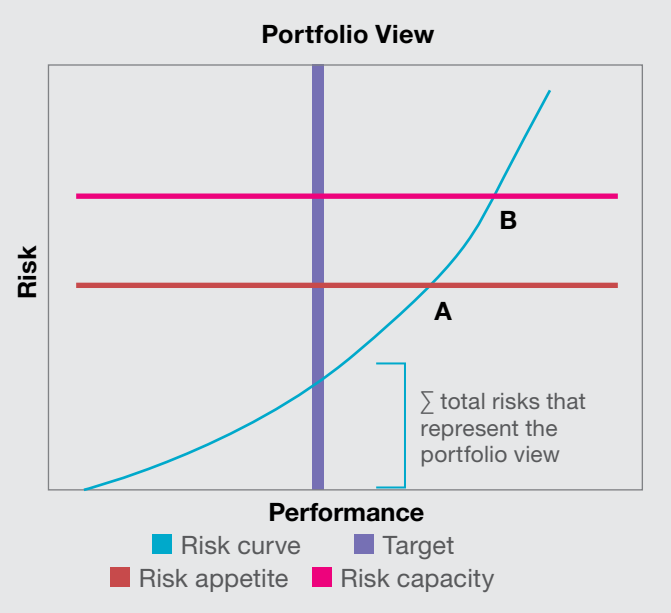
Figure C.10: Effect of Risk Response

Developing a Portfolio View

460. After selecting risk responses, management develops a composite assessment of risks that reflects the unit's residual risk profile relative to its business objectives and acceptable variation in performance. This forms an entity-wide risk profile or portfolio view of the risks facing the entity.

461. The portfolio view allows the organization to consider the type, severity, and interdependencies of risks, and how they may affect performance. Through the portfolio view, the organization identifies severe entity-level risks. Figure C.11 illustrates how the portfolio view can be depicted graphically.

Figure C.11: Portfolio View Using Risk Profile



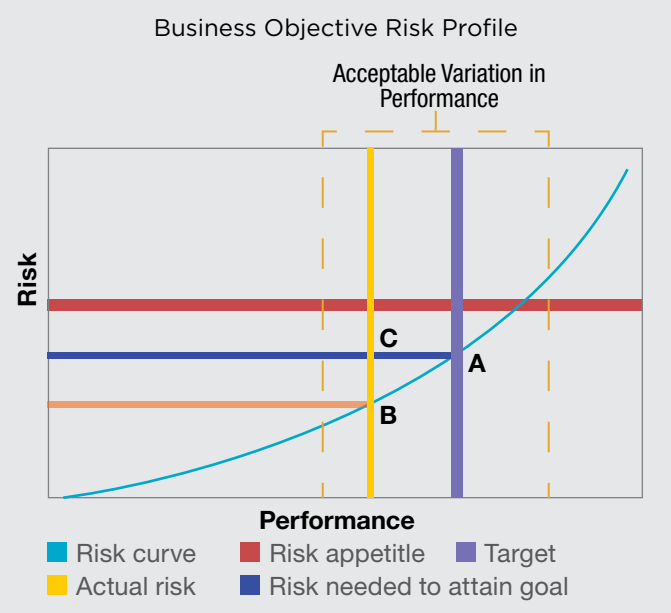
462. When preparing a risk profile that shows the portfolio view, the organization will typically use both qualitative and quantitative techniques. Quantitative techniques include regression modeling and other means of statistical analysis to determine the sensitivity of the portfolio to sudden or large changes. Qualitative techniques include scenario analysis and benchmarking. These changes may be represented as shifts in the position of the risk curve, or changes in gradient. Analysis may also identify the point on the curve where change becomes a disruption to the performance of the entity. For example, a financial institution identifies that a drop of more than 25% in market indices represents a disruptive change where the entity exceeds its risk appetite and impacts 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 impact 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).

463. 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 to challenge the assumptions underpinning the selection of the entity's strategy and assessment of the risk profile.

Monitoring Enterprise Risk Management Performance

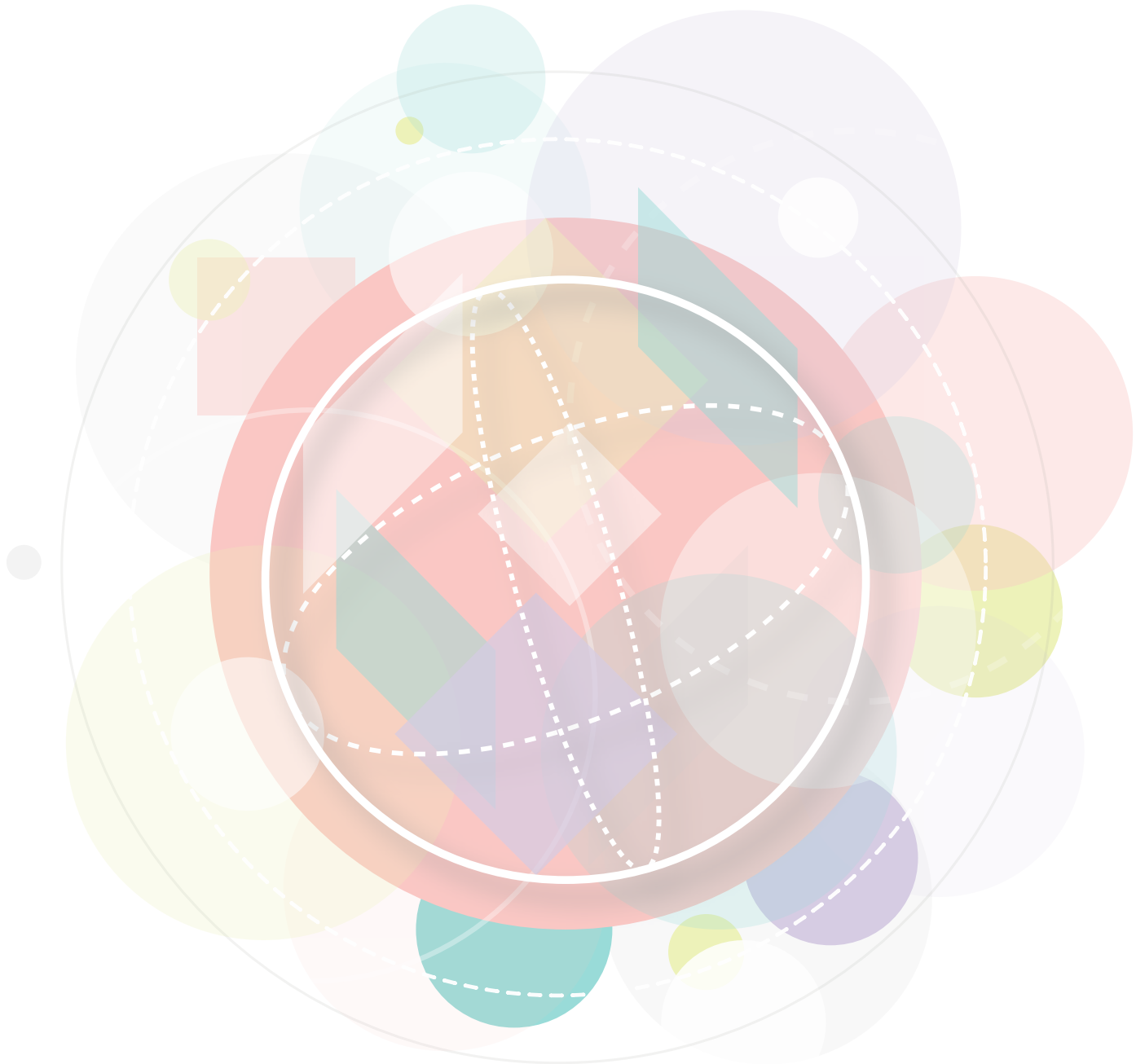
464. Organizations can use graphical representations to understand how risk is impacting performance. As shown in Figure C.12, management analyzes the risk profile to determine whether the current level of performance risk is greater, less than, or as expected compared to the risk assessment results. 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 C.12: 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.

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



To submit comments on this Public Exposure Draft, please visit www.erm.coso.org. Responses are due by **September 15, 2016**. Respondents will be asked to respond to a series of questions. Those questions may be found on-line at www.erm.coso.org and in a separate document provided at the time of download. Respondents may upload letters through this site. Please do not send responses by fax.

Written comments on the exposure draft will become part of the public record and will be available on-line until **December 31, 2016**.