COSO

Committee of Sponsoring Organizations of the Treadway Commission

Enterprise Risk Management

Integrating with Strategy and Performance

June 2017

Volume I

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

Robert B. Hirth Jr.
COSO Chair

Richard F. Chambers
The Institute of Internal Auditors

Mitchell A. Danaher
Financial Executives International

Charles E. Landes
American Institute of Certified Public Accountants

Douglas F. Prawitt
American Accounting Association

Sandra Richtermeyer
Institute of Management Accountants

PwC—Author

Principal Contributors

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

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

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

Matthew Bagin
Director
Washington DC, USA

Hélène Katz
Director
New York, USA

Katie T. Sylvis
Director
Washington DC, USA

Sallie Jo Perraglia
Manager
New York, USA

Kathleen Crader Zelnik
Manager
Washington DC, USA

Maria Grimshaw
Senior Associate
New York, USA

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 both boards and executives 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 to meet the demands of an evolving business environment. It is a concise framework for applying enterprise risk management within any organization to increase management and stakeholder confidence.

The updated document, now titled *Enterprise Risk Management–Integrating with Strategy and Performance*, highlights the importance of considering risk in both the strategy-setting process and in driving performance. The first part of the updated publication offers a perspective on current and evolving concepts and applications of enterprise risk management. The second part, the Framework, is organized into five easy-to-understand components that accommodate different viewpoints and operating structures, and enhance strategy and decision-making. In short, this update:

- Provides greater insight into the value of enterprise risk management when setting and carrying out strategy.
- Enhances alignment between performance and enterprise risk management to improve the setting of performance targets and understanding the impact of risk on performance.
- 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 proliferation of data and analytics in supporting decision-making.
- Sets out core definitions, components, and principles for all levels of management involved in designing, implementing, and conducting enterprise risk management practices.

Readers may also wish to consult a complementary publication, COSO's *Internal Control–Integrated Framework*. The two publications are distinct and have different focuses; neither supersedes the other. However, they do connect. *Internal Control–Integrated Framework* encompasses internal control, which is referenced in part in this updated publication, and therefore the earlier document 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 *Enterprise Risk Management–Integrating with Strategy and Performance*. 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 and Global and APA Risk and Regulatory Leader

Table of Contents

Applying the Framework:
Putting It into Context

1. Introduction

Integrating enterprise risk management practices 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 risk. The diligence required to integrate enterprise risk management provides an entity with a clear path to creating, preserving, and realizing value.

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 risk in the pursuit of value. The concepts and principles of enterprise risk management set out in this publication apply to all entities regardless of legal structure, size, industry, or geography.

Risk affects an organization's ability to achieve its strategy and business objectives. Therefore, one challenge for management is determining the amount of risk[2] the organization is prepared and able to accept. Effective enterprise risk management helps boards and management to optimize outcomes with the goal of enhancing capabilities to create, preserve, and ultimately realize value.

Management has many choices in how it will apply enterprise risk management practices, and no one approach is universally better than another. Yet, for any entity, one approach may provide increased benefits versus another or have a greater alignment with the overall management philosophy of the organization. This Framework sets out a basic conceptual structure of ideas, which an organization integrates into other practices occurring within the entity. Readers who are looking for information beyond a framework, or for different practices they can apply to integrate the enterprise risk management concepts into the entity, will find the appendices in Volume II to this publication helpful.

Enterprise Risk Management Affects Value

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, eroded, or realized.

- Value is *created* when the benefits derived from resources deployed exceed the cost of those resources. For example, value is created when a new product is successfully designed and launched and its profit margin is positive. 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,

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

2 In this publication, "risks" (plural) refers to one or more potential events that may affect the achievement of objectives. "Risk" (singular) refers to all potential events collectively that may affect the achievement of objectives.

service, and production capacity, which results in satisfied and loyal customers and stakeholders.

- Value is *eroded* when management implements a strategy that does not yield expected outcomes or fails to execute day-to-day tasks. For example, value is eroded when substantial resources are consumed to develop a new product that is subsequently abandoned.
- Value is *realized* when stakeholders derive benefits created by the entity. Benefits may be monetary or non-monetary.

How value is created depends on the type of entity. For-profit entities create value by successfully implementing a strategy that balances 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, integrating enterprise risk management practices with other aspects of the business enhances trust and instills greater confidence with stakeholders.

Mission, Vision, and Core Values

Mission, vision, and core values[3] define what an entity 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 through setting strategy, they are typically reaffirmed. Yet, they also may evolve as the expectations of stakeholders change. For example, a new executive management team may present different ideas for the mission to create value to the entity.

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.

- **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.

Enterprise Risk Management Affects Strategy

"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 throughout the entity.

Enterprise risk management[4] does not create the entity's strategy, but it influences its development. An organization that integrates enterprise risk management practices into setting strategy provides management with the risk information it needs to consider alternative strategies and, ultimately, to adopt a chosen strategy.

3 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.

4 Throughout this document, "enterprise risk management" refers to the culture, capabilities, and practices, integrated with strategy-setting and performance, that organizations rely on to manage risk in creating, preserving, and realizing value. It does not refer to a function, group, or department within an entity. Specific considerations on the operating model are discussed in Appendix B in Volume II.

Enterprise Risk Management Is Linked to Business

Enterprise risk management practices integrate with all other aspects of the business, including governance, performance management, and internal control practices.

Governance

Governance forms the broadest concept. Typically, this refers to the allocation of roles, authorities, and responsibilities among stakeholders, the board, and management. Some aspects of governance fall outside enterprise risk management (e.g., board member recruiting and evaluation; developing the entity's mission, vision, and core values).

Performance Management

Performance relates to actions, tasks, and functions to achieve, or exceed, an entity's strategy and business objectives. Performance management focuses on deploying resources efficiently. It is concerned with measuring those actions, tasks, and functions against predetermined targets (both short- and long-term) and determining whether those targets are being achieved. Because a variety of risks—both known and unknown—may affect an entity's performance, a variety of measures may be used:

- Financial measures, such as return on investments, revenue, or profitability.
- Operating measures, such as hours of operation, production volumes, or capacity percentages.
- Obligation measures, such as adherence to service-level agreements or regulatory compliance requirements.
- Project measures, such as having a new product launch within a set period of time.
- Growth measures, such as expanding market share in an emerging market.
- Stakeholder measures, such as the delivery of education and basic employment skills to those needing upgrades when they are out of work.

There is always risk associated with a predetermined performance target. For example, large-scale agriculture producers will have a certain amount of risk relating to their ability to produce the volumes required to satisfy customer demands and meet profitability targets. Similarly, airlines will have a certain amount of risk relating to their ability to operate all flights on schedule. Yet, airline companies may foresee less risk that they can operate 90% or even 80% of their scheduled flights on time versus 100% of their scheduled flights. In both of these examples, there is an amount of risk associated with managing to achieve the predetermined targets of performance—production volume and flight operation.

An entity can enhance its overall performance by integrating enterprise risk management into day-to-day operations and more closely linking business objectives to risk.

Internal Control

Enterprise risk management incorporates some concepts of internal control. "Internal control" is the process put into effect by an entity to provide reasonable assurance that objectives will be achieved. Internal control helps the organization to identify and analyze the risks to achieving those objectives and how to manage risks. It allows management to stay focused on the entity's operations and the pursuit of its performance targets while complying with relevant laws and regulations. Note, however, that some concepts relating to enterprise risk management are not considered within internal control (e.g., concepts of risk appetite, tolerance, strategy, and objectives are set within enterprise risk management but viewed as preconditions of internal control).

To avoid redundancy, some concepts relating to internal control that are common to both this publication and *Internal Control—Integrated Framework* have not been repeated here (e.g., fraud risk relating to financial reporting objectives, control activities relating to compliance objectives, and ongoing and separate evaluations relating to operations objectives). However, some common concepts relating to internal control are further developed in the Framework[5] section (e.g., governance of enterprise risk management). Please review *Internal Control–Integrated Framework*[6] as part of applying the Framework in this publication.

Benefits of Enterprise Risk Management

An organization needs 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 organization in creating value. In short, it must integrate enterprise risk management practices with strategy-setting and performance management practices, and in doing so it will realize benefits related to value.

Benefits of integrating enterprise risk management 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 and future opportunities. For example, when the managers of a locally based 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 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).
- *Increase positive outcomes and advantage while reducing negative surprises*: Enterprise risk management allows an organization to improve its ability to identify risks and establish appropriate responses, increasing positive outcomes while reducing negative 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 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 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).

5 "Framework" refers collectively to the five components introduced in Chapter 5 and covered individually in Chapters 6 through 10.

6 *Internal Control–Integrated Framework* can be obtained through www.coso.org.

- *Identify and manage entity-wide risks*: Every entity faces myriad risks that can impact many parts of the entity. Sometimes a risk can originate in one part of the entity but affect 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 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 ten minutes early as when it is ten 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. This helps 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 affect 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 helps to optimize 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 significant additional resources over a longer period of time.

Keep in mind that the benefits of integrating enterprise risk management practices with strategy-setting and performance management practices will vary by entity. There is no one-size-fits-all approach available for all entities. However, implementing enterprise risk management practices 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

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 the achievement of strategy and business objectives.

Because risk is always present and always changing, pursuing and achieving 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, resilience, and agility. The Framework incorporates this concept in the broad context of creating, preserving, and realizing value.

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. Example 1.1 illustrates such a plan in practice.

Example 1.1: Crisis Management Plan

A cruise ship operator is concerned about 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 practices. First, routine on-board cleaning and sanitizing are 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 forty-eight hours. By having strong enterprise risk management practices 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.

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 noted in Example 1.1, which affects only a few passengers, the fire affects everyone. There may be an immediate need for medical assistance, food, water, and shelter, or even a call to off-load all 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 hours of a port or another cruise ship. This overlap allows the company to rapidly redeploy ships and crews to assist in an emergency.

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 create value.

2. Understanding the Terms: Risk and Enterprise Risk Management

Defining Risk and Uncertainty

An entity's strategy and business objectives may be affected by potential events. A lack of complete predictability of an event occurring (or not) and its related impact creates uncertainty for an organization. Uncertainty exists for any entity[7] that 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.*

The box on this page contains terms that expand on and support the definition of risk. The Framework 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 expected event that does not occur.

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

In the context of risk, events are more than routine transactions; they include broader business matters such as changes in the governance and operating structure, geopolitical and social influences, and contracting negotiations, among other things. Some events that potentially affect strategy and business objectives are readily discernable—a change in interest rates, a competitor launching a new product, or the retirement of a key employee. 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.

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,[8] such as better-than-forecast weather, stronger staff retention trends, or improved tax rates, which should 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 has a positive effect on financial performance. However, it may also increase risk to the supply chain, which may result in unsatisfied customers if the company cannot supply the product.

Some risks have minimal impact on an entity, and others have a larger impact. Enterprise risk management practices help the organization identify, prioritize, and focus on those risks that may prevent value from being created, preserved, and realized, or that may erode existing value. But, just as important, it also helps the organization pursue potential opportunities.

7 "Entity" is a broad term that can encompass a wide variety of legal structures including for-profit, not-for-profit, and governmental entities.

8 This Framework distinguishes between positive outcomes and opportunities. Positive outcomes relate to those instances where performance exceeds the original target. Opportunities relate to an action or potential action that creates or alters goals or approaches for creating, preserving, and realizing value.

Defining Enterprise Risk Management

Enterprise risk management is defined here as:

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

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

- Recognizing culture.
- Developing capabilities.
- Applying practices.
- Integrating with strategy-setting and performance.
- Managing risk to strategy and business objectives.
- Linking to value.

Recognizing Culture

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 decisions and 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 make decisions while understanding that culture plays an important role in shaping those decisions.

Developing Capabilities

Organizations pursue various competitive advantages to create value for the entity. Enterprise risk management adds to the skills needed to carry out 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 and opportunities.

Applying Practices

Enterprise risk management is not static, nor is it an adjunct to a business. Rather, it is continually 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.

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 they are expected to manage risk. In turn, this understanding supports decision-making at all levels and helps to reduce organizational bias.

Integrating with Strategy-Setting and Performance

An organization sets strategy that aligns with and supports 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 understanding the overall risk profile for the entity and the implications of alternative strategies to that risk profile. Management specifically considers any new opportunities that arise through innovation and emerging pursuits.

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 core operations of the entity, management is likely to identify new opportunities to grow the business.

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 enterprise risk management practices with an entity's operating activities, and understanding how risk potentially impacts the entity overall, not just in one area, enterprise risk management can become more effective.

Managing Risk to Strategy and Business Objectives

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 risk of achieving strategy and business objectives is appropriate for that entity, recognizing that no one can predict risk with absolute precision.

But even with reasonable expectations in place, entities can experience unforeseen challenges, which is why regularly reviewing enterprise risk management practices is important. Review—and consequent revision when needed—helps maintain robust practices that increase management's confidence in the entity's ability to successfully respond to the unexpected and achieve its strategy and business objectives.

Linking to Value

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. The first expression of risk appetite is an entity's mission and vision. Different strategies will expose an entity to different risks or different amounts of similar risks.

Risk appetite provides guidance on the practices an organization is encouraged to pursue or not pursue. It sets the range of appropriate practices and guides risk-based decisions rather than specifying a limit.

Risk appetite is not static; it may change between products or business units and over time in line with changing capabilities for managing risk. The types and amount of risk that an organization might consider acceptable can change. For example, during good economic times, a successful and growing company may be more willing to accept certain downside risk than when economic times are bad and business outlooks deteriorate. Risk appetite must be flexible enough to adapt to changing business conditions as needed without waiting for periodic management reviews and approvals.

While risk appetite is introduced here,[9] the Framework sets out numerous instances where it is applied as part of enterprise risk management. Some of the more important applications of risk appetite are its:

- Use by the organization in making decisions that enhance value.
- Help in aligning the acceptable amount of risk with the organization's capacity to manage risk and opportunities.
- Relevance when setting strategy and business objectives, helping management consider whether performance targets are aligned with acceptable amount of risk.
- Assistance in communicating risk profiles desired by the board.
- Relevance and alignment with risk capacity.
- Use in evaluating aggregated risk at a portfolio view.

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.

9 Risk appetite is discussed further in the Framework under Principle 7: Defines Risk Appetite.

3. Strategy, Business Objectives, and Performance

Enterprise Risk Management and Strategy

Enterprise risk management helps an organization better understand:

- How mission, vision, and core values form the initial expression of what types and amount of risk are acceptable to consider when setting strategy.
- The possibility that strategy and business objectives may not align with the mission, vision, and core values.
- The types and amount of risk the organization potentially exposes itself to by choosing a particular strategy.
- The types and amount of risk inherent in carrying out its strategy and achieving business objectives and the acceptability of this level of risk, and ultimately, value.

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

Figure 3.1: Strategy in Context

Possibility of Misaligned Strategy and Business Objectives

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. Consider the statements from a healthcare provider in Example 3.1.

These statements guide the organization in determining the types and amount of risk it is likely to encounter and accept. 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 being 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.

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

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 to which the organization is potentially exposed.

When evaluating potential risks that may arise from strategy, management also considers any critical assumptions that underlie the chosen strategy. These assumptions form an important part of the strategy and may relate to any of the considerations that form part of the entity's business context. 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.

Example 3.2 considers the mission and vision of the healthcare provider discussed earlier, and how the entity cascades these into its strategy statement. Using the statement shown in that example, 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 an approach the organization has not previously focused on. These and many other risks result from the choice of strategy. Yet, 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 set goals.

Example 3.1: Cascading 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, and compassion, while holding them accountable for these values.

Example 3.2: Cascading Mission, Vision, and Core Values

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.

Risk to Implementing the Strategy and Business Objectives

There is always risk to carrying out a 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.

The risk to carrying out strategy may also be viewed through the lens of business objectives. An organization can use a variety of techniques to assess risks using some kind of common measure. Wherever possible, the organization should use similar units for measuring risk for each objective. Doing so will help to align the severity of the risk with established performance measures.

Enterprise Risk Management and Performance

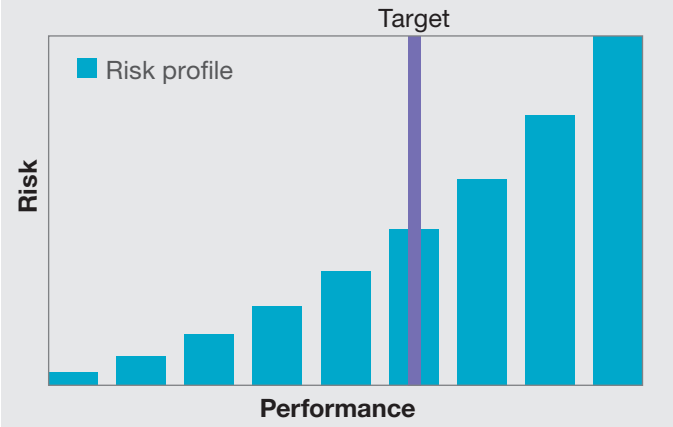
Assessing risk to the strategy and business objectives requires an organization to understand the relationship between risk and performance—referred to in this Framework as the "risk profile." An entity's risk profile provides a composite view of the risk at a particular level of the entity (e.g., overall entity level, business unit level, functional level) or aspect of the business model (e.g., product, service, geography).

This composite view allows management to consider the type, severity, and interdependencies of risks, and how they may affect performance. The organization should initially understand the potential risk profile when evaluating alternative strategies. Once a strategy is chosen, the focus shifts to understanding the current risk profile for that chosen strategy and related business objectives.

The relationship between risk and performance is rarely linear. Incremental changes in performance targets do not always result in corresponding changes in risk (or vice versa). Consequently, a useful, dynamic representation, 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.

There are several methods for depicting a risk profile. The Framework uses one approach, shown here, to illustrate the relationship between various aspects of enterprise risk management. Doing so helps to enhance the conversations of risk, risk appetite, tolerance, and the overall relationship to performance targets.

Figure 3.2: Risk Relative to Performance



In Figure 3.2, each bar represents the aggregate amount of risk for a specific level of performance for a business objective. The 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. Organizations may develop different approaches for conceptualizing and depicting the entity's risk profile.

Risk profiles that trend upwards, as shown in Figure 3.2, are typical of, but not limited to, business objectives such as:

- *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.
- *Recruitment of specialist resources:* As entities pursue increasingly niche products or markets, the risks associated with attracting and retaining expertise and experience in their workforce increases.
- *Transportation and logistics:* As the number of locations or volume of goods increases, the size of the transportation fleet and complexity of operations grows, resulting in a higher amount of risk.
- *Funding for capital works and improvements:* In illiquid markets, or where consumer confidence is low, the amount of risk associated with an entity's ability to secure funding for capital works, projects, or initiatives increases.

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 the intrinsic relationship between risk, targeted performance, and actual performance.

Risk profiles help management to determine what amount of risk is acceptable and manageable in the pursuit of strategy and business objectives. Risk profiles[10] may help management:

- Understand the level of performance in the context of the entity's risk appetite (see Principle 7: *Defines Risk Appetite*).
- Find the optimal level of performance given the organization's ability to manage risk (see Principle 9: *Formulates Business Objectives*).
- Determine the tolerance for variation in performance related to the target (see Principle 9: *Formulates Business Objectives*).
- Assess the potential impact of risk on predetermined targets (see Principle 11: *Assesses Severity of Risk* and Principle 14: *Develops Portfolio View*).

While the risk profile shown here implies needing a specific level of precision, and perhaps data to create, keep in mind that it can also be developed using qualitative information.

10 Refer to Appendix D in Volume II for a more detailed discussion on risk profiles.

4. Integrating Enterprise Risk Management

The Importance of Integration

An entity's success is the result of countless decisions made every day by the organization that affect the performance and, ultimately, the achievement of the strategy or business objectives. Most of those decisions require selecting one approach from multiple alternatives. Many of the decisions will not be simply either "right" or "wrong," but will include trade-offs: time versus quality; efficiency versus cost; risk versus reward.

When making such decisions, management and the board must continually navigate a dynamic business context, which requires integrating enterprise risk management thinking into all aspects of the entity, at all times. The Framework, therefore, views enterprise risk management in just that way. It is not simply a function or department within an entity, something that can be "tacked on." Rather, culture, practices, and capabilities are, together, integrated and applied throughout the entity.

Integrating enterprise risk management with business activities and processes results in better information that supports improved decision-making and leads to enhanced performance. In addition it helps organizations to:

- Anticipate risks earlier or more explicitly, opening up more options for managing the risks and minimizing the potential for deviations in performance, losses, incidents, or failures.
- Identify and pursue existing and new opportunities in accordance with the entity's risk appetite and strategy.
- Understand and respond to deviations in performance more quickly and consistently.
- Develop and report a more comprehensive and consistent portfolio view of risk, thereby allowing the organization to better allocate finite resources.
- Improve collaboration, trust, and information sharing across the organization.

Integration enables the organization to make decisions that are better aligned with the speed and potential disruption of individual risks and the pursuit of new opportunities. Risk-aggressive entities may need to obtain risk-related information quickly and have streamlined decision-making processes in place in order to pursue fast-moving opportunities. For example, consider an investment firm that has been presented with an opportunity to bid on a new deal, but is required to respond within several hours. The firm's risk management practices are well integrated with the capabilities within the bidding process, allowing the organization to collect and review the available information and make a decision in the time required.

Where risk management practices and capabilities are separate, collecting relevant information, identifying stakeholders, and making decisions all take longer, and that can jeopardize an entity's ability to meet urgent deadlines. In short, the more risk aggressive the entity, the greater the value of integration.

Toward Full Integration

For most entities, integrating enterprise risk management is an ongoing endeavor. Factors that influence integration are entity culture, size, complexity, and how long a risk-aware culture has been embraced.

An entity that is just beginning to develop enterprise risk management will have limited practices and capabilities on which to rely. But as the entity matures, it implements more dedicated practices and capabilities that improve decision-making (such as identifying, assessing, and responding to risks). Once organizations consistently integrate risk considerations, they become less reliant on the formalized, stand-alone practices and infrastructure. For example, in a fully integrated entity, personnel will identify deviations in performance and understand the potential effect on the risk profile without relying on a stand-alone assessment program.

Time isn't the only factor affecting an entity's ability to fully integrate enterprise risk management. Size and type matter, too (i.e., whether the entity is for profit, not-for-profit, heavily regulated, etc.). For example, a large pharmaceuticals company may have a well-developed risk-aware culture, but may be required to retain some stand-alone monitoring and reporting practices by its regulators. In comparison, smaller non-regulated entities may focus more on developing risk awareness and integrating risk throughout performance reporting.

In a fully integrated entity, enterprise risk management practice will also affect the operating structure. At this point, awareness and responsibility for risk are more evenly distributed across the operating structure, which is often characterized by the understanding that "everyone is a risk manager." Silos of knowledge are broken down to enable better decision-making across the entity.

The following lists provide examples of how organizations can foster full integration of enterprise risk management throughout the culture, capabilities, and practices of the entity, with the result being better decision-making.

Culture

Instilling more transparency and risk awareness into an entity's culture requires actions such as:

- Implementing forums or other mechanisms for sharing information, making decisions, and identifying opportunities.
- Encouraging people to escalate issues and concerns without fear of retribution.
- Clarifying and communicating roles and responsibilities for the achievement of strategy and business objectives, including responsibilities for the management of risk.
- Aligning core values, behaviors, and decision-making with incentives and remuneration models.
- Developing and sharing a strong understanding of the business context and drivers of value creation.

Capabilities

Enterprise risk management capabilities are integrated into the entity when:

- Management is able to make decisions that are appropriate given its appetite, risk profile of the entity, and the changes to the profile that occur over time.
- The organization routinely hires capable individuals with relevant experience who can exercise judgment and oversight in accordance with their responsibilities.
- The organization has access to capable individuals, subject matter experts, or other technical resources to support decision-making.
- When making necessary investments in technology or other infrastructure, management considers the tools required to enable enterprise risk management responsibilities.
- Vendors, contractors, and other third parties are considered in discussions of risk and performance.

Practices

Enterprise risk management practices are integrated when:

- Setting strategy explicitly considers risk when evaluating options.
- Management actively addresses risk in pursuit of its performance targets.
- Activities are developed to regularly and consistently monitor performance results and changes in the risk profile throughout the entity.
- Management is able to make decisions that are in line with the speed and scope of changes in the entity.

Example 4.1 describes integration in practice.

Example 4.1: Integration in Practice

The management of a large government department integrates enterprise risk management practices with the monthly performance management meetings. At these meetings, they analyze performance and discuss new, emerging, and changing risks that affect their ability to effectively serve the public. This promotes greater transparency and increased responsiveness to the most important risks, sharing of ideas on how best to approach the risk, and greater consistency on deploying risk responses across the operations of the department.

Addressing Integration in the Framework

Each component of enterprise risk management includes principles (set out in the following chapter), which apply to creating, preserving, and realizing value in an organization regardless of size, type, or location. The principles and their components do not represent isolated, stand-alone concepts. Each highlights the importance of integrating enterprise risk management and the role of decision-making.

For each principle, the Framework outlines considerations to fully integrating culture, practices, and capabilities into the entity. These considerations are not exhaustive, but they do demonstrate the range of inputs into decision-making and the exercise of judgment by personnel, management, and the board.

5. Components and Principles

Components and Principles of Enterprise Risk Management

The Framework 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. The three ribbons in the diagram of Strategy and Objective-Setting, Performance, and Review and Revision represent the common processes that flow through the entity. The other two ribbons, Governance and Culture, and Information, Communication, and Reporting, represent supporting aspects of enterprise risk management.

The figure further illustrates that when enterprise risk management is integrated across strategy development, business objective formulation, and implementation and performance, it can enhance value. Enterprise risk management is not static. It is integrated into the development of strategy, formulation of business objectives, and the implementation of those objectives through day-to-day decision-making.

Figure 5.1: Risk Management Components

The five components[11] are:

- **Governance and Culture:** Governance and culture together form a basis for all other components of enterprise risk management. Governance sets the entity's tone, reinforcing the importance of enterprise risk management, and establishing oversight responsibilities for it. Culture is reflected in decision-making.
- **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 effect on 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.
- **Performance:** An organization identifies and assesses risks that may affect an entity's ability to achieve its strategy and business objectives. As part of that pursuit, the organization identifies and assesses risks that may affect the achievement of that strategy and business objectives.

11 Components are discussed in detail in Chapters 6 through 10.

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 entity-level business objectives.

- **Review and Revision:** By reviewing enterprise risk management capabilities and practices, and the entity's performance relative to its targets, an organization can consider how well the enterprise risk management capabilities and practices have increased value over time and will continue to drive value in light of substantial changes.
- **Information, Communication, and Reporting:** Communication is the continual, iterative process of obtaining information and sharing it 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. By using information that applies to all components, the organization reports on risk, culture, and performance.

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: Risk Management Principles

Assessing Enterprise Risk Management

An organization should have a means to reliably provide to the entity's stakeholders with a reasonable expectation that it is able to manage risk to an acceptable amount. 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 provides criteria for conducting an assessment and determining whether the enterprise risk management culture, capabilities, and practices collectively manage the risk of not achieving the entity's strategy and supporting business objectives. During an assessment, the organization considers 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.
- The controls necessary to put into effect relevant principles are present and functioning.[12]

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

In these three considerations, being "present" means the components, principles, and controls exist in the design and implementation of enterprise risk management to achieve strategy and business objectives. Being "functioning" means they continue to operate to achieve strategy and business objectives. And "operating together" refers to the interdependencies of components and how they function cohesively. Organizations may place different emphasis on specific principles and apply them differently, depending on the benefits an organization seeks to attain through enterprise risk management.[13] When these components, principles, and supporting controls are present and functioning, the organization can reasonably expect that enterprise risk management is helping the entity create, preserve, and realize value.

Different approaches are available for assessing enterprise risk management. When the assessment is performed to communicate to external stakeholders, it would be conducted considering the principles set out in the Framework. When assessing enterprise risk management for internal purposes, some organizations may choose to use some form of maturity model in completing this evaluation, recognizing that the model must be tailored to address the complexity of the business. Factors that add 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.

During an assessment, management may also review the suitability of those capabilities and practices, keeping in mind the entity's complexity and the benefits the organization seeks to attain through enterprise risk management.

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

Framework

6. Governance and Culture

Principles Relating to Governance and Culture

1. **Exercises Board Risk Oversight:**
   The board of directors provides oversight of the strategy and carries out governance responsibilities to support management in achieving strategy and business objectives.
2. **Establishes Operating Structures:**
   The organization establishes operating structures in the pursuit of strategy and business objectives.
3. **Defines Desired Culture:**
   The organization defines the desired behaviors that characterize the entity's desired culture.
4. **Demonstrates Commitment to Core Values:**
   The organization demonstrates a commitment to the entity's core values.
5. **Attracts, Develops, and Retains Capable Individuals:**
   The organization is committed to building human capital in alignment with the strategy and business objectives.

Introduction

An entity's board of directors plays an important role in governance and significantly influences enterprise risk management. 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.

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.

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 core values: the beliefs, attitudes, desired behaviors, and importance of understanding risk. Culture supports the achievement of the entity's mission and vision. An entity with a culture that is risk-aware 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 governance responsibilities to support management in achieving strategy and business objectives.

Accountability and Responsibility

The board of directors has the primary responsibility for risk oversight in the entity, and in many countries it has a fiduciary responsibility to the entity's stakeholders, including conducting reviews of enterprise risk management practices. Typically, the full board is responsible for risk oversight, leaving the day-to-day responsibilities of managing risk to management. Some full boards retain ownership while others delegate board-level responsibilities to a committee of the board, such as a risk committee. Regardless of the structure, it is common to develop a statement that defines the board's and management's respective responsibilities.

Skills, Experience, and Business Knowledge

The board of directors is well positioned to offer expertise and provide oversight of enterprise risk management 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, and performance targets. It also includes interacting with stakeholders and presenting alternative views and actions.

Risk oversight is possible only when the board understands the entity's strategy and industry, and stays informed on relevant issues. As the business context changes, so does risk 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 oversight. For example, entities exposed to cyber risk may need to have board members who either have expertise in information technology or access to the required expertise through independent advisors.

Example 6.1: Factors That Impede Board Independence

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 capacity by the organization.
- 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 organization.
- Has donated a significant financial amount to an entity.
- Has business or personal relationships with key stakeholders within an organization.
- Sits as a board member of other organizations that represent a potential conflict of interest.
- Has held the same board position for an extended period.

Independence

The board overall should be independent. Independence enhances directors' ability 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 director's ability to be objective (see Example 6.1).

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.

While independence is often a larger focus within publicly traded companies, similar considerations apply to private entities, government bodies, and not-for-profit entities.

Suitability of Enterprise Risk Management

It is important that the board understand the complexity of the entity and how integrating enterprise risk management capabilities and practices will enhance value. The board engages in conversations with management to determine whether enterprise risk management is suitably designed to enhance value.

For example, some organizations may derive value from 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. Others may gain value from aligning 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 increasing the range of opportunities in support of that strategy.

Organizational Bias

Bias in decision-making has always existed and always will. It is not unusual to find within an entity evidence of 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 affecting decisions relating to 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 Operating Structures

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

An operating structure describes how the entity organizes and carries out its day-to-day operations. Through the operating structure, 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 structure contributes to managing risk to the strategy and business objectives.

The operating structure is typically aligned with the legal structure and management structure. The legal structure influences how an entity operates and the management structure sets out the reporting lines, roles, and responsibilities for ongoing management and operation of the business.

Different legal structures may be more or less suitable depending on the 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 decisions may become segregated if risk information is not aggregated across legal structures.

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.

Operating Structure and Reporting Lines

The organization establishes an operating structure and designs reporting lines to carry out the strategy and business objectives. It is important for the organization to clearly define responsibilities when designing reporting lines. The organization may also enter into relationships with external third parties that can influence reporting lines (e.g., strategic business alliances, outsourcing, or joint business ventures).

Different operating structures may result in different perspectives of a risk profile, which may affect enterprise risk management practices. For example, assessing risk within a decentralized operating structure 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.

Factors to consider when establishing and evaluating operating structures 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.

The organization considers these and other factors when deciding what operating structure to adopt. 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.

Enterprise Risk Management Structures

Management plans, organizes, and carries out 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 example of a commonly used 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.

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 structure and reporting lines, which allows management to make business decisions as needed, with a full understanding of the risks embedded in those decisions.

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. In some small entities, enterprise risk management oversight may be less formal, with management being much more involved in day-to-day decisions.

Authority and Responsibilities

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, and functions aligned to strategy and business objectives.

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

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[14] is often 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.

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

14 The chief risk officer is the individual who is 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."

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 responsibility 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 business partner is not taken on without exercising due diligence).

Enterprise Risk Management within the Evolving Entity

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 structure to change as the nature of the business and its strategy evolves. Management, therefore, regularly evaluates the operating structure and associated reporting lines.

In today's world of evolving information technology, new operating structures are emerging. It may be that standard operating structures soon become "virtual" in nature, relying far less on physical locations and more on technological interconnections. This will require examining how risk will 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 structure and understand how changes due to innovation will influence enterprise risk management practices.

Principle 3: Defines Desired Culture

The organization defines the desired behaviors that characterize the entity's desired culture.

Culture and Desired Behaviors

An organization's culture reflects its core values, behaviors, and decisions. Decisions are in turn a function of the available information, judgment, capabilities, and experience. 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.

It is up to the board of directors and management to define the desired culture of the entity as a whole and of the individuals within it. The core values drive the expected behaviors in day-to-day decision-making in order to meet the expectations of stakeholders. Establishing a culture embraced by all personnel—where people do the right thing at the right time—is critical to the organization being able to seize opportunities and manage risk to achieve the strategy and business objectives.

Many factors shape entity culture. Internal factors include, among other things, the level of judgment and autonomy provided to personnel, 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 other elements.

All these factors influence where the entity positions itself 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 differing types and greater amount of risk to achieve strategy and business objectives (see Example 6.2).

Figure 6.1: Culture Spectrum

A well-defined 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 maintaining full compliance well within the desired risk appetite. Working separately, these two units could adversely affect the entity, but by having a shared understanding of acceptable risk decisions, they can respond appropriately within the defined risk appetite to achieve the strategy and business objectives.

Applying Judgment

Judgment has a significant role in defining the desired culture and management of risk across the culture spectrum. Judgment is often relied upon:

- When there is limited information or data available to support a decision.
- Where there are unprecedented changes in the strategy, business objectives, performance, or risk profile of the organization.
- During times of disruption.

Judgment is a function of personal experiences, risk appetite, capabilities and the level of information available, and organizational bias. Management judgment is susceptible to bias whenever over- or under-confidence in the organization's abilities exist, for example, or anchoring assumptions and attributing correlations are based on limited information. Behaviors within the entity may also lead to organizational bias that affects judgment. Group dynamics in meetings, communication styles of management, and recognition and acknowledgment of personnel may affect the ability of management to exercise good judgment.

Example 6.2: Two Ends of the Culture Spectrum

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.

In contrast, a private equity manager is more 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.

The use of judgment influences the ability of an organization to navigate periods of crisis and resume normal operations more efficiently. During periods of disruption, the ability for an organization to function in accordance with existing policies or procedures may be hampered, requiring it to rely more on the judgment and behaviors of management and the board. The actions taken by the organization to steer the entity out of a crisis depend on the accountability, behaviors, and actions of personnel. Organizations with management teams who have extensive experience, established capabilities, and well-defined risk appetite will likely exercise judgment with greater clarity. Stakeholders are in turn likely to have greater confidence that the organization will recover successfully when the judgment demonstrated is in line with the core values of the entity.

Judgment also affects the extent to which innovation and the identification of opportunities are fostered within an entity. When the entity is characterized by very prescriptive practices and limited delegations of authority, innovation may be stifled. An organization that places a stronger emphasis on risk-aware culture may rely more on management's judgment when making decisions that enhance values and in seeking new opportunities in line with the risk appetite of the entity.

Effect of Culture

The culture of an organization affects how risk is identified, assessed, and responded to from the moment of setting strategy through to execution and performance. Examples include:

- *Scoping of strategy and business objective-setting:* The culture of an organization may affect the types of strategic alternatives being considered. For example, despite promising feasibility studies, a risk-averse organization may choose not to expand mining and drilling operations into new geographies.

- *Applying rigor to the risk identification and assessment processes:* Depending where an organization sits on the culture spectrum, the nature and types of risks and opportunities may differ. What are viewed as potential risks by a risk-averse entity may be considered as opportunities worthy of pursuit by another. For example, increasing demand for online ordering may be seen as a risk for a traditional retail manufacturer but as an opportunity to increase sales by a retailer looking to grow sales and market share.
- *Selecting risk responses and allocating finite resources:* A risk-averse entity may allocate risk responses or additional resources in order to gain higher confidence of the achievement of a specific business objective. The costs and benefits associated with incremental risk responses may be interpreted less favorably by more risk-aggressive entities. For example, purchasing additional insurance may be favored by risk-averse entities, but may be viewed as an inefficient use of financial resources by another.
- *Reviewing performance:* Trends in the risk profile or business context may be addressed differently by entities on different points of the culture spectrum. A risk-averse entity may make changes more quickly to risk responses as variations in performance are identified. Entities that are more risk aggressive may wait longer before making changes or may make smaller changes. For example, airlines may adjust flight schedules more quickly in response to adverse changes in weather conditions than train or bus companies, which may be able to continue operating without disruption for longer.

Aligning Core Values, Decision-Making, and Behaviors

The ability for an organization to successfully achieve its strategy and business objectives is impeded when the behaviors and decisions of the organization do not align with its core values. Misalignment can result in a loss of confidence from stakeholders, inconsistent approaches, and lower than targeted performance.

When core values 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, and strategy.
- Risk is an afterthought to strategy-setting and business planning.
- Performance targets create incentives or pressures that instill behavior contrary to core values.
- There is no clear escalation policy on important risk and performance matters.
- The investigation and resolution of excessive risk-taking is inadequate.
- Management or other personnel deliberately act in a way that does not comply with core values.

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 more consistently aligned with the entity's risk appetite.

Shifting Culture

Culture does not stay constant over time (see Example 6.3). Changes within the organization and external influences may cause an entity's culture to shift. 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. Mergers and acquisitions can also result in changes to the culture. These changes will affect how the organization looks at risk and influence how decisions are made.

Example 6.3: When Deviations to Standards of Conduct Occur

A technology start-up is developing a new algorithm that improves the accuracy of tracking changes in customer behaviors and purchasing preferences. In its infancy, the start-up had a very aggressive risk culture as it worked through the initial phases of establishing commercial operations and identifying potential business partners, customers, and market opportunities. As the organization matured it entered into more formal partnerships with larger clients. The start-up eventually decided to become publicly listed to access a larger group of investors. With this change, the company shifted to the left on the culture spectrum, which mirrored the company's risk appetite and corresponding changes to the enterprise risk management practices and capabilities of the entity.

Principle 4: Demonstrates Commitment to Core Values

The organization demonstrates a commitment to the entity's core values.

Reflecting Core Values throughout the Organization

Understanding the entity's core values is fundamental to enterprise risk management. Core values are reflected in actions and decisions applied across the entity. Without a strong and supportive understanding of, and commitment to, those values communicated from the top of the organization, risk awareness can be undermined and risk-inspired decisions may be inconsistent with those values. The manner in which values are communicated across the organization is often referred to as the "tone" of the organization.

A consistent tone establishes 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 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 the performance of enterprise risk management responsibilities in the pursuit of the entity's strategy and business objectives will be.

Aligning the culture and tone of the organization gives confidence to stakeholders that the entity is adhering to its core values and the pursuit of its mission and vision. For example, in an entity where "safety first" is a core value, management demonstrates its commitment by actively encouraging everyone at every level to identify and escalate safety practices regardless of their role in the organization. External stakeholders such as safety inspectors who observe the content and tone of training materials, internal communications, and reporting will consequently have the confidence that the organization is embracing its culture and core values.

Embracing a Risk-Aware Culture

Management defines the characteristics needed to achieve the desired culture over time, with the board providing oversight and focus. An organization can then 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 team or department 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.
- *Aligning risk-aware behaviors and decision-making with performance:* Remuneration and incentive programs are aligned to the core values of the organization including expected behaviors, adherence to codes of conduct, and promoting accountability for risk-aware decision-making and judgment.

- *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, and understands that managing risk is 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.

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 should lead by example to reflect its 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 in line with its core values.

Enforcing Accountability

The board of directors ultimately holds the chief executive officer[15] 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 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.

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 and a common purpose.

Accountability is evident in the following ways:

- Management and the board of directors clearly communicating the expectations (e.g., developing and enforcing standards of conduct).
- 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 committing 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).

15 The Framework refers to "chief executive officer." Other terms describing this senior leadership position that may be used include "chief executive," "president," "managing director," or "deputy."

Holding Itself Accountable

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 the core values and desired culture behaviors 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.

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

Keeping Communication Open and Free from Retribution

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.

Information is shared and escalated to the relevant level within the entity. Transparency of information may relate to:

- Changes in the understanding of assumptions underpinning the selection of a strategy or business objectives.
- Ongoing adequacy of a risk response.
- Incidents, failures, errors, or unexpected losses.
- Variations in performance including overperformance, including those facilitated by third parties.
- Changes in the risk profile or portfolio view of risk of the entity.
- Deviations in expected behaviors compared to the core values of the organization.

In addition, management provides the board of directors with an appropriate level 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 issues with management.

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 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.

Responding to Deviations in Core Values and Behaviors

If establishing a culture in which management and personnel act according to desired behaviors is fundamental to enterprise risk management, then why do things sometimes go wrong? Even in those entities that solidly demonstrate a commitment to their core values, operational failures, scandals, and crises do sometimes occur—damaging reputations and ultimately leaving an organization unable to achieve its strategy and business objectives.

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

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 6.4).

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 to being put on probation to even being terminated. In all cases, the expectations of risk-aware behavior, judgment, and decision-making must remain consistent. Consistency ensures that the entity's culture is not undermined.

Example 6.4: When Deviations to Core Values Occur

For a global pharmaceutical company, research and development (R&D) is often one of the biggest costs, as products may take ten to twenty years to develop and bring to market and require 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, thereby impeding management from making an informed decision on moving from drug trials to production, and the drug is launched, there could be severe effects to the entity if patients who use the drug experience adverse side effects. Moreover, R&D's failure to disclose would likely be a clear violation of the desired conduct of the company.

Principle 5: Attracts, Develops, and Retains Capable Individuals

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

Establishing and Evaluating Competence

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 the management and personnel of each of the 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.

The human resources function helps promote competence by assisting management in 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

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 desired 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 business context.
- *Evaluate:* Measure the performance of individuals in relation to achieving business objectives and demonstrating enterprise risk management competence against 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.

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.

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?

Rewarding Performance

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.

Salary increases and bonuses are common incentives, but non-monetary rewards such as being given greater responsibility, visibility, and recognition are also effective. Management consistently applies and regularly reviews the entity's measurement and reward structures in conjunction with its 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 6.5).

Example 6.5: Performance, Incentives, and Rewards

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 units' production goals and the expectation to comply with all safety and quality standards, workplace safety laws, customer loyalty programs, and accurate product recall reporting. Once they aligned business objectives with incentives and rewards, the company noted in the staff a greater sense of accountability and more willingness to work together to address challenges, and ultimately there was a measurable decline in product defects.

Addressing Pressure

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 change in business context, such as a sudden dip in the economy, can also add pressure.

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, individuals may circumvent processes or engage in fraudulent activity. Organizations can positively influence pressure by rebalancing workloads or increasing resource levels, as appropriate, and continue to communicate the importance of ethical behavior.

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 6.6).

Pressure is also created by change: change in strategy, in operating structure, 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.

Example 6.6: The Price of Pressure

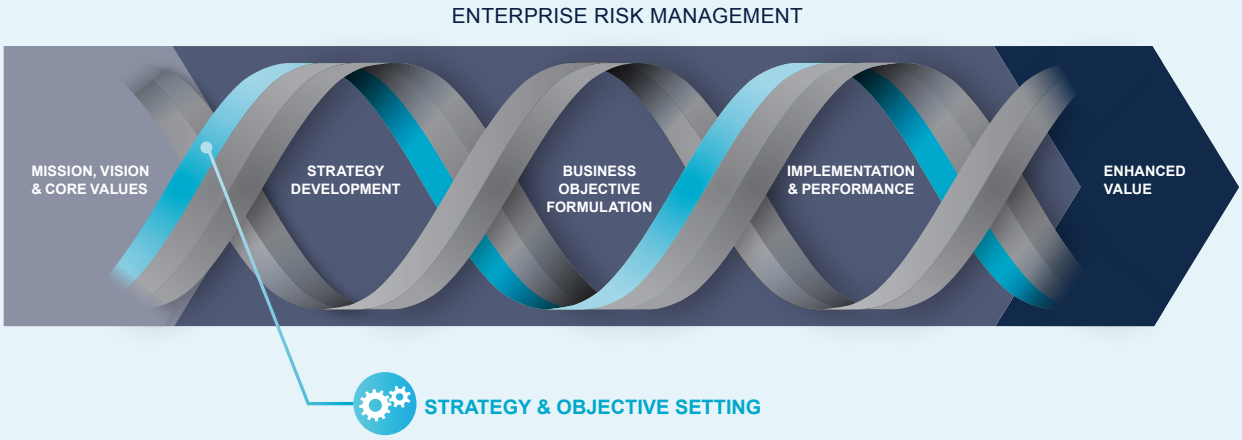
Possible negative reaction to pressure should be accounted for when considering compensation and incentives. For example, investment managers take risks on behalf of their clients, and the performance of those investment portfolios may significantly affect the entity's remuneration. A fee based on fund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

Preparing for Succession

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. Strategy and Objective-Setting

Principles Relating to Strategy and Objective-Setting



6. **Analyzes Business Context:**
   The organization considers potential effects of business context on risk profile.
7. **Defines Risk Appetite:**
   The organization defines risk appetite in the context of creating, preserving, and realizing value.
8. **Evaluates Alternative Strategies:**
   The organization evaluates alternative strategies and potential impact on risk profile.
9. **Formulates Business Objectives:**
   The organization considers risk while establishing the business objectives at various levels that align and support strategy.

Introduction

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 the strategy 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 the business objectives. Doing so guides the organization and helps to sharpen the strategy and the tasks necessary to carry it out.

Principle 6: Analyzes Business Context

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

Understanding Business Context

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 an organization's current and future strategy and business objectives. Business context may be:

- Dynamic, where new risks can emerge at any time disrupting 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, where change happens quickly and in unanticipated ways (e.g., currency fluctuations and political forces).

Considering External Environment and Stakeholders

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

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 may be in a better position to anticipate and adapt to change.

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.).

The external environment comprises several factors that can be categorized by the acronym PESTLE: political, economic, social, technological, legal, and environmental (see Figure 7.1). Example 7.1 provides a scenario to illustrate this concept.

Example 7.1: External Environment Influences

Two competing global technology companies are both seeking to increase revenues. The first company is considering launching an established product in developing countries, while the other company is developing a new product that would expand its existing consumer base. 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 supply chain considerations. In contrast, the second company focuses on social and technological factors as it seeks to understand changing customer needs. Even though both companies are in the same industry, they have different external environments that influence their specific risk profiles and their chosen strategy.

Figure 7.1: External Environment Categories and Characteristics[16]

Categories	External Environment Characteristics
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, GDP growth, 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/or industry standards
Environmental	Natural or human-caused catastrophes, ongoing climate change, changes in energy consumption regulations, attitudes toward the environment

Considering Internal Environment[17] and Stakeholders

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.

Figure 7.2: Internal Environment Categories and Characteristics

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

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

17 Internal environment is explored in detail in the Governance and Culture component (Chapter 6).

How Business Context Affects Risk Profile

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 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 might evolve in relation to where it is heading or wants to head. Example 7.2 illustrates how an organization can consider business context within the components of enterprise risk management.

Example 7.2: Considering Business Context in Each of the Framework Components

The management of a retail company integrates understanding of business context with other enterprise risk management practices as follows:

- **Governance and Culture:** The organization develops an understanding of governance and associated regulatory trends. The board incorporates this understanding of emerging expectations into its oversight of enterprise risk management practices.
- **Strategy and Objective-Setting:** Management conducts a detailed analysis of social trends, retail trends, and consumer confidence levels driving behavior of its core customer base and incorporates findings into its strategic-setting cycle for long-term value and success.
- **Performance:** Management incorporates its understanding of environmental trends and how they may affect the assessment of risks relating to the objective of reducing packing by 50% in line with its core values.
- **Review and Revision:** Management considers how changes in workforce practices, namely the emergence of the mobile workforce, may also affect the entity's culture and enterprise risk management practices, including opportunities to enhance current practices.
- **Information, Communication, and Reporting:** Management considers that legislation concerning information privacy may affect the way the entity captures, communicates, and reports on risk information.

Principle 7: Defines Risk Appetite

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

Applying Risk Appetite

Decisions made in selecting strategy and developing risk appetite are not linear, with one decision always preceding the other. Nor is there a universal risk appetite that applies to all entities.

Many organizations develop strategy and risk appetite in parallel, refining each throughout strategy-setting. Some boards will provide input and may challenge management on its choice of risk appetite, while others will be expected to concur with management and approve the risk appetite set. Regardless of how the decisions are made, the organization would have a preliminary understanding of its risk appetite based on the established mission and vision and prior strategies. These are important inputs into any risk appetite, which is refined whenever an organization reviews alternative strategies and selects a desired strategy.

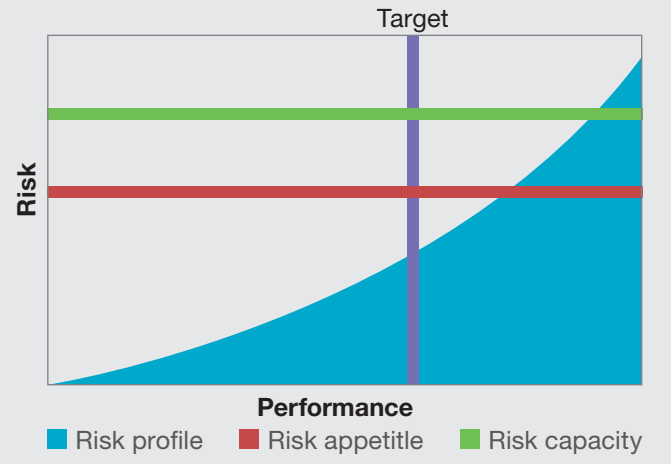
Some entities consider risk appetite in qualitative terms while others prefer to use quantitative terms, often focusing on balancing growth, return, and risk. Whatever the approach for describing risk appetite, it should reflect the entity's culture. Moreover, if the organization wants to change some aspect of the culture, defining a strong risk appetite can help create and reinforce that desired 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 seeking the optimal balance between risk and opportunity.

Taken together, these considerations help frame the entity's risk appetite and provide greater precision than a single, higher-level statement. Figure 7.3 depicts the risk profile as a solid area (in blue), filling the space across the performance axis from the individual risk profile bars (from the earlier illustration of Figure 3.2). A line showing risk appetite has also been added.

On any depiction of risk profile, organizations may also plot risk capacity (as in Figure 7.3), 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 choose to do so. This could happen, for instance, in the case of an organization accepting the threat of insolvency, understanding that success can create considerable value. Where the organization is managing risks above its risk appetite, management will typically be expected to either amend its practices to operate within its risk appetite or formally accept this level of risk taking, Some organizations will also seek board approval in such instances. (Additional discussion on risk profiles is presented in Appendix D in Volume II.)

Figure 7.3 Risk Profile Showing Risk Appetite and Risk Capacity



Determining Risk Appetite

There is no standard or "right" risk appetite that applies to all entities. Management and the board of directors choose a risk appetite with an informed understanding of the trade-offs involved. Risk appetite may encompass a single depiction or several depictions that align and collectively specify the acceptable types and amount of risk.

A variety of approaches are available to determine risk appetite, including facilitating discussions, reviewing past and current performance targets, and modeling. In determining risk appetite, organizations may consider stakeholders as noted in the discussion on business context. It is up to management to communicate the agreed-upon risk appetite at various levels of detail throughout the entity. With the support of the board, management also revisits and reinforces risk appetite over time in light of new and emerging considerations.

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. In some instances, organizations may develop quantitative measures that link to the risk appetite statement. Typically these measures would align with the strategy and related business objective targets. For instance, an entity that focuses its enterprise risk management practices on reducing performance variability may express risk appetite using financial results or the beta of its stock.

Risk appetite should be positioned and perceived as a dynamic approach for shaping the entity's risk profile rather than as an additional constraint on performance. For that reason, some entities will develop a series of cascading expressions of risk appetite referencing "targets," "ranges," "ceilings," or "floors" (see Example 7.3). Others will use specific quantitative terms as a way of increasing precision.

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.

Example 7.3: 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 0.50% 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 that 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 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.

- *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.

Management may also consider the entity's risk profile, risk capacity, enterprise risk management 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* is the maximum amount of risk the entity can absorb in pursuit of strategy and business objectives. 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

Some organizations articulate risk appetite as a single point; others as a continuum (see Example 7.4).

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[18] categories.
- Performance targets of the entity.

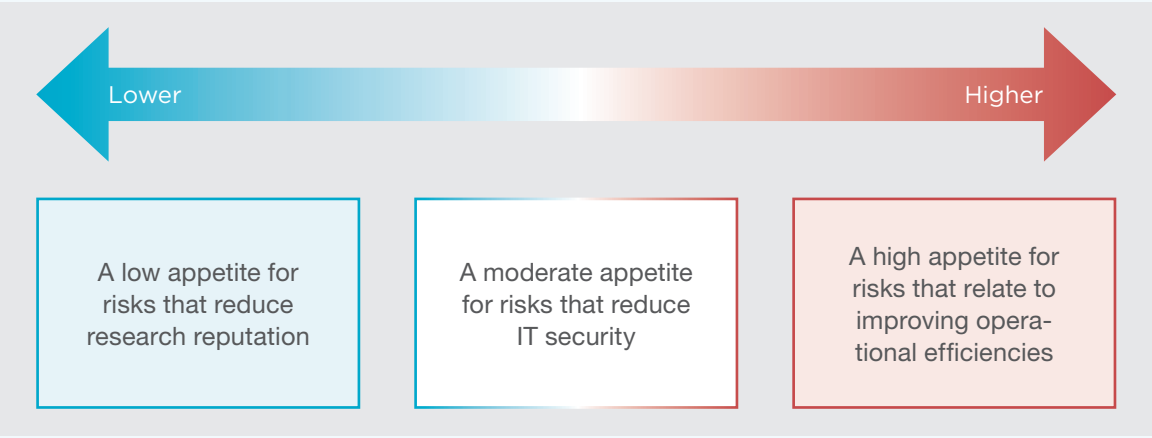
Some organizations will develop and articulate risk appetite using other approaches, such as risk categories. These approaches are sometimes easier to manage and assess. However, they can also result in organizations managing risk in silos rather than taking an integrated view of enterprise risk management.

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, especially those who perform tasks to achieve business objectives (e.g., local sales forces, country managers).

18 Formulating business objectives is discussed in Principle 9. They are included here to better illustrate how risk appetite cascades from strategy through business objectives.

Most organizations will choose to communicate risk appetite broadly across the entity. Some may choose to focus on senior roles that have direct responsibility for managing performance. This may occur, for instance, where there is sensitivity to competitor activity, access to private or confidential information, or potential for risk appetite to impede compliance with obligations. In some instances, organizations may also choose to communicate risk appetite to external stakeholders, either in its entirety or in an abbreviated form.

Example 7.4: Risk Appetite Expression



A university has set its strategy 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 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.

Example 7.5 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 7.5: Cascading Risk Appetite

Mission: To provide healthy, great-tasting premium organic foods made from locally sourced ingredients.

Vision: To be the largest producer of sustainably 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 have a lower risk appetite for making any decisions that challenge our brand. We will not make decisions that put cost above our core values, product quality, or ingredient choice. Nor will we make decisions that put growth above sustainable operations. However, we will strive to be innovative to develop products that meet customers' preferences and accept risk viewed as moderately severe (or less) that leads to impacts on brand.

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. We understand that such a focus has a more moderate risk profile and will manage the risk of failing to develop new tastes our customers desire with the opportunity to enhance our product offerings.

Risk Appetite: We will not make decisions that 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 have a lower risk appetite relating to decisions impacting our retail presence. We will only accept risks that impact retail presence where we believe that we can increase the long-term value of the company and those retailers share our values. We understand that making decisions in this manner may affect our sales channel.

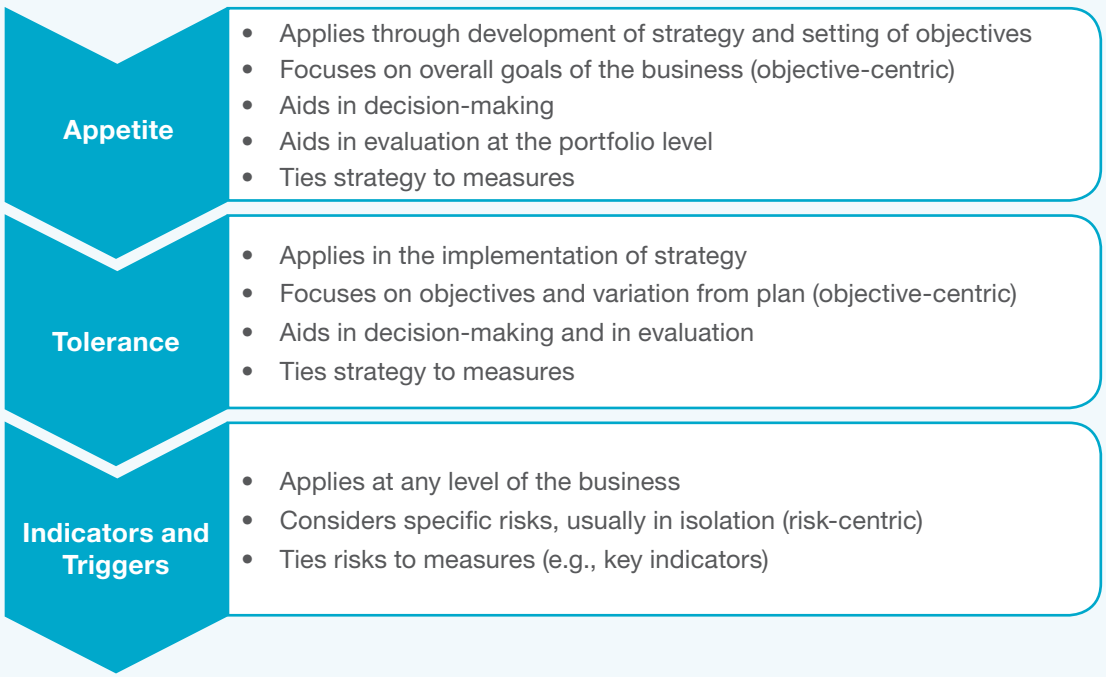
Using Risk Appetite

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. For instance, management may choose to allocate a greater portion of resources to those business objectives with a lower risk appetite versus those business objectives with a higher risk appetite. The organization seeks to align people, processes, and infrastructure to successfully implement strategy and business objectives while remaining within its risk appetite.

Risk appetite is incorporated into decisions on how the organization operates. 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.

But risk appetite is only part of the approach. To fully embed risk appetite into decision-making at various levels, it does need to cascade through and align with other practices. Figure 7.4 depicts this important relationship and the application of risk appetite, tolerance,[19] and indicators and triggers[20] as they cascade within an entity.

Figure 7.4 Risk Appetite, Tolerance, and Limits and Triggers



19 Tolerance is discussed later in this chapter in Principle 9.

20 Limits and triggers are discussed in the Performance component.

Principle 8: Evaluates Alternative Strategies

The organization evaluates alternative strategies and potential impact on risk profile.

An organization must evaluate alternative strategies as part of strategy-setting and assess the risk and opportunities of each option. 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: (1) the possibility that the strategy does not align with the mission, vision, and core values of the entity, and (2) the implications from the chosen strategy.

The Importance of Aligning Strategy

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

Further, a misaligned strategy increases risk to stakeholders because the value of the organization and its reputation may be affected. For example, consider a telecommunications company that 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 effect to its reputation with community groups and regulators that insist that services be maintained.

Understanding the Implications from Chosen Strategy

When evaluating alternative strategies, the organization seeks to identify and understand the potential risks and opportunities 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. In some instances, this evaluation may need to consider multiple strategies to understand the potential dependency of one strategy on another.

Another consideration when evaluating alternative strategies is the supporting assumptions relating to business context, resources, and capabilities. These assumptions are an important part of the strategy. They may relate to any of the internal and external considerations that form part of the entity's business context. Where assumptions are unproven, there is often a higher risk of disruption than there would be if the organization had 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 affect 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 or where the assumptions are largely unproven.

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

The amount of effort expended and the level of precision required to evaluate alternative strategies will vary by the significance and complexity of the decision, the resources and capabilities available, and the number of strategies being evaluated. The more significant or complex the decision, the more detailed the evaluation will be, perhaps using several approaches.

Popular approaches to evaluating alternative strategies are SWOT analysis,[21] modeling, valuation, revenue forecast, competitor analysis, and scenario analysis. The evaluation is typically performed by management 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.

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 7.6 illustrates one organization's approach for evaluating the possibility of alternative strategies not aligning with mission and vision and implications from the alternative strategies on the entity's risk profile. This example also illustrates the need to understand competing priorities between customers, employees, and shareholders.

Aligning Strategy with Risk Appetite

An organization should expect that the strategy it selects can be carried out 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, it needs to be revised, an alternative strategy selected, or the risk appetite revisited.

For instance, a sports equipment 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."

The development of risk appetite should align with the development of strategy and business plans, otherwise it may appear that goals and priorities are conflicting, or even creating tensions on the types and amounts of risk reflected in decision-making.

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

Example 7.6: Considering Alternative Strategies

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 the strategy-setting process, several alternatives are assessed.

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.

- 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 midsized 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.

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.

	Business Objective	Performance Measure and Target
Alternative 1	• Possibility of operating in such a manner that quality and safety are not aligned with the company's core values	• Risk that additional variability in operations may affect customer satisfaction and erode value • Risk that increased complexity of operations (e.g., regulations, tax laws, foreign exchange rates) may impact efficiency of operations
Alternative 2	• Possibility of operating in a manner that weather may represent difficult working conditions for staff and equipment, and impact safety of operations	• Risk that the company cannot maintain high-quality year-round transportation services, which means customer satisfaction would be affected
Alternative 3	• Possibility of operating in a manner that increased costs may erode shareholder returns	• Risk of operating in a manner where investing in high-quality transportation practices increases costs and impacts shareholder returns

Making Changes to Strategy

Typically, organizations hold periodic strategy-setting sessions to outline both short-term and long-term strategies. 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 boundary of risk it is willing to accept, or requires 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 7.7).

Example 7.7: Making Changes to Strategy

A global camera manufacturer used to sell film cameras, but as digital cameras became more popular, the company started to experience 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.

Mitigating Bias

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 strategy-setting. Where such bias exists, the organization should take steps to mitigate that bias. 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 9: Formulates Business Objectives

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

Establishing Business Objectives

The organization develops business objectives that are specific, 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.

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

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.

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 carrying out other business objectives.

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 effect on the risk profile. A business objective that results in the organization exceeding the risk appetite may be modified or, perhaps, discarded.

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 from Chosen Business Objectives

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 enter 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.

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 7.8).

Example 7.8: Determining the Implications of a Chosen Business Objective

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. Given the importance of maintaining financial performance, the organization chooses to abandon the selected business objectives.

Categorizing Business Objectives

Many organizations will group common business objectives into common categories. Some organizations will categorize or group business objectives to align with specific aspects of the strategy, such as market share, customer focus, or corporate responsibility. Organizations may also align business objectives with various business groups of the entity, such as operations, human resources, or other defined functional areas. Regardless of how they are categorized, they must align with business practices, products, geographies, or other organizational dimensions. How an organization categorizes its business objectives is decided by management.

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.

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

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 forty minutes.
- A call center endeavors to minimize missed calls to 2% of overall calls received.

By setting targets, the organization is able to influence the risk profile of the entity. An aggressive target may result in greater risk for that business objective. For example, an organization may set aggressive growth targets that heighten the risks in pursuing added growth. Conversely, an organization may set a more conservative growth target that will lower the risk of not achieving the target, but may also result in the target no longer aligning with the achievement of the business objective.

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 performance. 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 reviewing the appropriateness of the performance measures and targets are discussed in Chapter 8.)

Example 7.9 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.

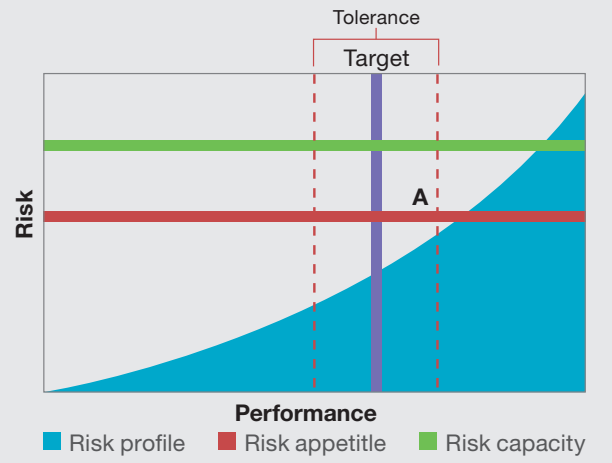
Example 7.9: Sample Business Objectives by Level

	Business Objective	Performance Measure and Target
Business objectives (entity)	• Continue to develop 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 Confectionary (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

Understanding Tolerance

Closely linked to risk appetite is tolerance—the acceptable variation in performance. 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.

Figure 7.5 Risk Profile Showing Tolerance



Having an understanding of the tolerance for 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 maximum point where the performance target could be set is where the right boundary of tolerance intersects with risk appetite ("A" in Figure 7.5).

Unlike risk appetite, which is broad, tolerance 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 tolerance, 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 range of tolerance. Tolerance focuses on objectives and performance, not specific risks.

Operating within defined tolerance 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 Established Tolerances

Performance measures related to a business objective help confirm that actual performance is within an established tolerance (see Example 7.10). Performance measures can be either quantitative or qualitative. Tolerance 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.

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.

Example 7.10 Trailing Target Variation

A large beverage bottler sets a target of having no more than five lost-time incidents in a year and sets the tolerance 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.

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 7.11).

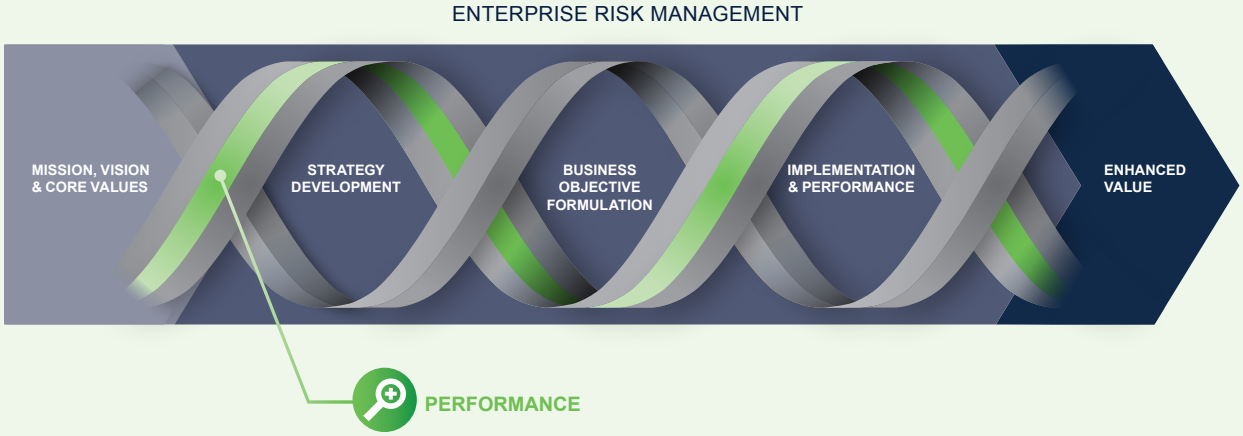
Organizations should also understand the relationship between cost and tolerance so they can deal effectively with associated risk. Typically, the narrower the tolerance, the greater amount of resources required to operate within that level of performance. Consider airlines, for example, which track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

Example 7.11: Tolerance Statements

Business Objective	Target	Tolerance
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

8. Performance

Principles Relating to Performance



10. **Identifies Risk:**
    The organization identifies risk that impact the performance of strategy and business objectives.
11. **Assesses Severity of Risk:**
    The organization assesses the severity of risk.
12. **Prioritizes Risks:**
    The organization prioritizes risks as a basis for selecting responses to risks.
13. **Implements Risk Responses:**
    The organization identifies and selects risk responses.
14. **Develops Portfolio View:**
    The organization develops and evaluates a portfolio view of risk.

Introduction

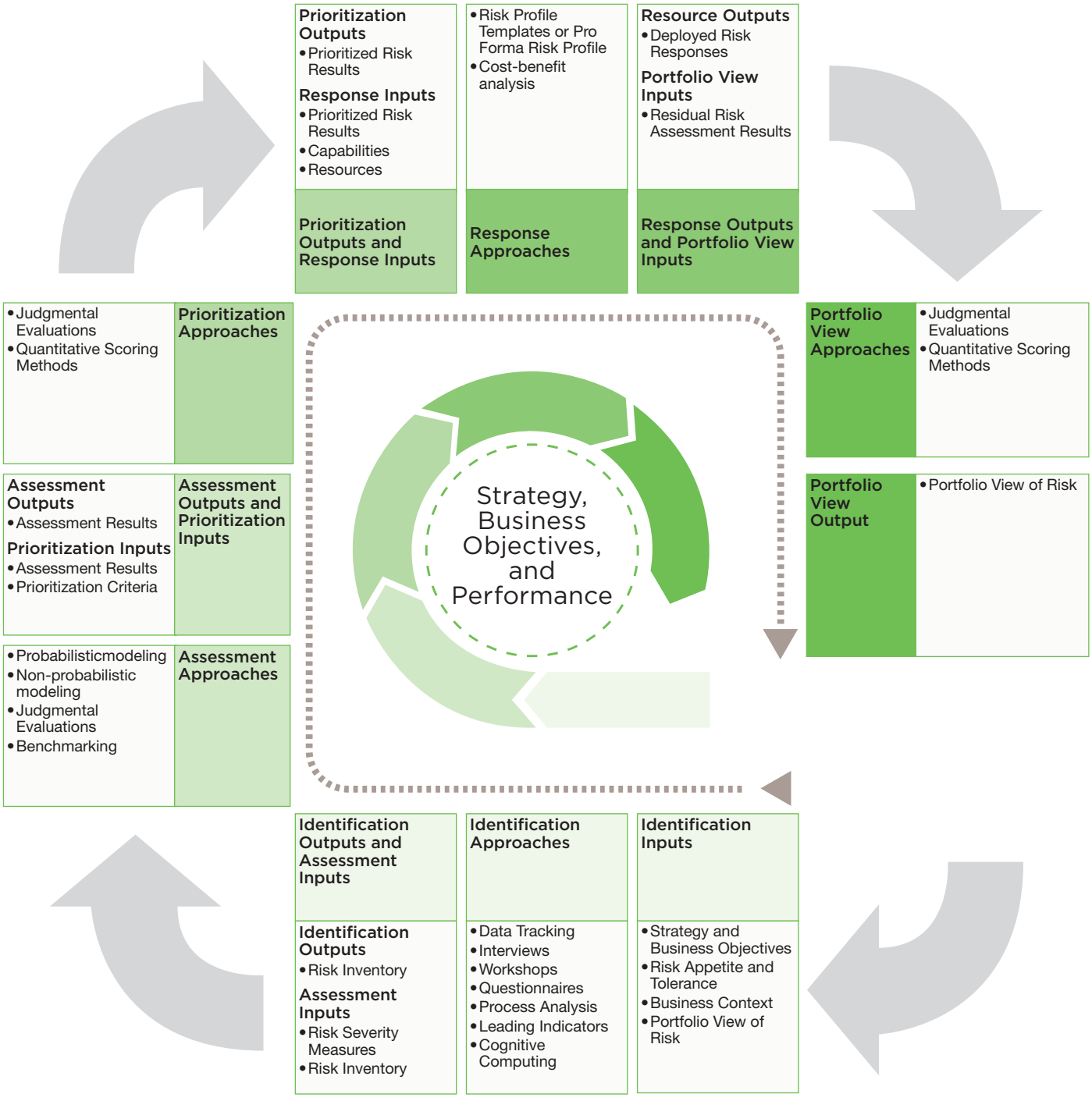
Creating, preserving, realizing, and minimizing the erosion of an entity's value is further enabled by identifying, assessing, and responding to risk that may impact the achievement of the entity's strategy and business objectives. Risks originating at a transactional level may prove to be as disruptive as those identified at an entity level. Risks may impact one operating unit or the entity as a whole. They 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, a range of responses is required from across the entity and at all levels.

This component of the Framework focuses on practices that support the organization in making decisions and achieving strategy and business objectives. To that end, organizations use their operating structure to develop a practice 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 entity-level business objectives.

Figure 8.1 illustrates that these practices are iterative, with the inputs in one step of the process typically being the outputs of the previous step. The practices are 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



Principle 10: Identifies Risk

The organization identifies risk that impacts the performance of strategy and business objectives.

Identifying Risk

The organization identifies new, emerging, and changing risks to the achievement of the entity's strategy and business objectives. It undertakes risk identification activities to first establish an inventory of risks, and then to confirm existing risks as being still applicable and relevant. As enterprise risk management practices are progressively integrated, the knowledge and awareness of risks is kept up-to-date through normal day-to-day operations. Some entities will supplement those activities from time to time in order to confirm the completeness of the risk inventory. How often an organization does this will depend on how quickly risks change or new risks emerge. Where risks are likely to take months or years to materialize, the frequency at which risk identification occurs will be less than where risks are less predictable or will occur at a greater speed.

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 operations).
- Were previously identified but have since been altered due to a change in the business context, risk appetite, or supporting assumptions (e.g., a positive increase in the expected sales forecasts affecting production capacity).

Emerging risks 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 initially assess accurately, and may warrant re-identification more frequently. Additionally, organizations should communicate evolving information about emerging risks.

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

Some risks may remain unknown—risks for which there was no reasonable expectation that the organization would consider during risk identification. These 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.

Organizations want to identify those risks that are likely to disrupt operations and affect 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 affect the relevance and longevity of existing products and services.
- *Expanding role of big data and data analytics:* How organizations can effectively and efficiently access, transform, and analyze large volumes of structured and unstructured data sources.
- *Depleting natural resources:* The diminishing availability and increasing cost of natural resources that affect 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 activities 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.
- *Political environment:* Actions by a government that alter operations of an industry in a country.

Embedded in identifying risk is identifying opportunities.[22] 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 to renew the workforce to better pursue growth. Similarly, advances in technology may represent a risk to distribution and service models for retailers as well as an opportunity to change how retail customers obtain goods (e.g., through online service). Where opportunities are identified, they are communicated through the organization to be considered as part of setting strategy and business objectives.

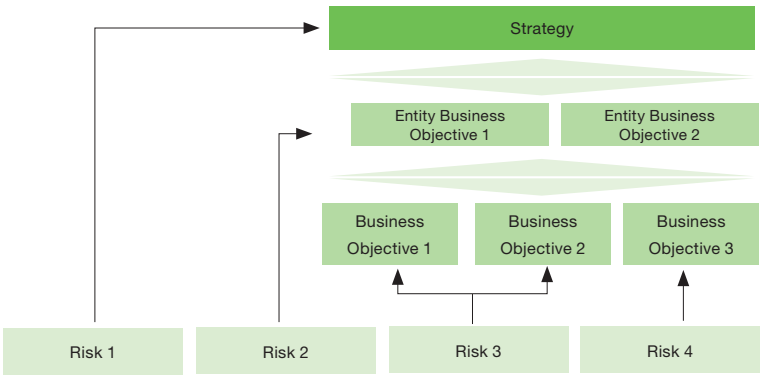
Using a Risk Inventory

A risk inventory is simply a listing of the risk the entity faces. Depending on the number of individual risks identified, organizations may structure the risk inventory by category to provide standard definitions for different risks. This allows similar risks to be grouped together, such as financial risks, customer risks, or compliance (or more broadly, obligation) risks. Within each category, organizations may choose to further define risks into more detailed sub-categories. The risk inventory can be updated to reflect changes identified by management.

Figure 8.2 illustrates how risks that impact different levels of the entity form part of the risk inventory:

- Risk 1 potentially impacts the strategy directly.
- Risk 2 impacts the entity business objectives.
- Risk 3 impacts multiple business objectives that then aggregate and impact entity business objectives.
- Risk 4 impacts a single business objective and that also impacts entity business objectives.

Figure 8.2: Risk Impacts at Differing Levels



22 This Framework distinguishes between positive events and opportunities. Positive events are those instances where performance exceeds the original target. Opportunities are actions or potential actions that create or alter goals or approaches for creating, preserving, and realizing value.

Because the impact of risks cannot be limited to specific levels or functions, identification activities should capture all risks, and regardless of where they are identified, all risks form part of the entity's risk inventory. For example, an entity that identifies risks at the strategy level relating to board governance and achieving diversity targets must also consider these risks at a business objective level. Or an organization that identifies the risk of missing a customer billing deadline at a business objective level should consider the impact of that risk at the entity level.

To demonstrate that a comprehensive risk identification has been carried out, management will identify risks and opportunities across all functions and levels—those risks 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.

Approaches to Identifying Risk

A variety of approaches are available for identifying risks. The organization can identify risks as part of day-to-day activities such as budgeting, business planning, performance reviews, and meetings as considerations in the approval processes for new products and designs and in response to customer complaints, incidents, or financial losses. Identification activities integrated through the entity can be supplemented by additional targeted activities such as simple questionnaires, facilitated workshops, and interviews. Some approaches may be enabled by technology, such as data tracking and complex analytics.

Depending on the size, geographic footprint, and complexity of an entity, management may use more than one technique. For example, an entity may collect internal data on historical incidents and losses and analyze it to identify new, emerging, and changing risks. Additionally, the nature and type of the risk may determine the appropriate technique. For example, management may use more sophisticated approaches to identify risks associated with an acquisition. 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 identifying different types of risks.

Figure 8.3: Approaches for Identifying Risks

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

- *Cognitive computing* allows organizations to collect and analyze large volumes of data to detect future trends and meaningful insights in new and emerging risks as well as changes in existing risks more efficiently than a human.
- *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.
- *Interviews* solicit the individual's knowledge of past and potential events. For canvassing large groups of people, questionnaires or surveys may be used.
- *Key indicators* are qualitative or quantitative measures that help to identify changes to existing risks. Risk indicators should not be confused with performance measures, which are typically retrospective in nature.

- *Process analysis* involves developing a diagram of a process to better understand the interrelationships of its inputs, tasks, outputs, and responsibilities. Once mapped, risks can be identified and considered against relevant business objectives.
- *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.

Whatever approaches are selected, an organization considers how changes in assumptions underpinning the strategy and business objectives may create new or emerging risks. For example, in one case management assumed an exchange rate on par with the local currency for importing raw materials. The actual exchange rate, however, declined by more than 10%, which created a new risk to meeting overall profitability targets. Additionally, management considered the business context—the expected economic outlook for the entity, changing customer preferences, and anticipated growth rates when conducting risk identification.

When identifying risks, the organization should aim to precisely describe the risk itself, rather than other considerations of that risk, such as the root causes of the risk, the potential impacts of the risk, or the effect of the risk being poorly implemented. Figure 8.4 compares descriptions of these other considerations, which are less helpful, to precise risk descriptions, which are preferred.

Figure 8.4: Describing Risks with Precision

Other Considerations	Imprecise Risk Descriptions	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 associated with a risk occurring	• New product is more successful than planned, production capacity struggles to keep up with increased demand, resulting in delivery delays, unhappy customers, and adverse effects on the company's reputation • The risk of denial of service attacks due to legacy IT systems that result in leaked customer data, regulatory penalties, loss of customers, and negative press	• The risk that demand exceeds production targets impacting customer service • The risk of denial of service attacks impacting the ability to retain the confidentiality of customer data
Potential effects of poorly implemented risk responses	• 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

Precise risk identification:

- Allows the organization to more effectively manage the risk inventory and understand its relationship to the business strategy, objectives, and performance.
- Allows the organization to more accurately assess the severity of the risk in the context of business objectives.
- Helps the organization identify the typical root causes and impacts, and therefore select and deploy the most appropriate risk responses.
- Allows the organization to understand interdependencies between risks and across business objectives.
- Supports the aggregation of risks to produce the portfolio view.

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

Framing Risk

Prospect theory, which explores human decision-making, says that individuals are not risk neutral; rather, a response to loss tends to be more extreme than a response to gain. And with this comes a tendency to misinterpret probabilities and best solution reactions. As well, how a risk is framed—focusing on the upside (a potential gain) or downside (a potential loss)—often will influence the response. With that in mind, consider the importance of describing risk with a consistent sentence structure to reduce framing bias. Example 8.1 presents an illustration of framing.

Example 8.1: Framing

An individual is confronted with two sets of choices:

1. A sure gain of $240, or a 25% chance to gain $1,000 and a 75% chance to gain nothing.
2. A sure loss of $750, or a 75% chance to lose $1,000 and a 25% chance to lose nothing.

In the first set, most people select "a sure gain of $240," because that is framed in the positive. In the second set, most people select a "75% chance to lose $1,000," because in this case it is the loss that is more certain. Prospect theory holds that people do not want to put at risk what they already have or think they can have, but they will have higher risk tolerance when they think they can minimize losses.

Principle 11: Assesses Severity of Risk

The organization assesses the severity of risk.

Assessing Risk

Risks identified and included in an entity's risk inventory are assessed in order to understand the severity of each to the achievement of an entity's strategy and business objectives. Risk assessments inform the selection of risk responses. Given the severity of risks identified, management decides on the resources and capabilities to deploy in order for the risk to remain within the entity's risk appetite.

Assessing Severity at Different Levels of the Entity

The severity of a risk is assessed at multiple levels (across divisions, functions, and operating units) in line with the business objectives it may impact. It may be that risks assessed as important at the operating unit level, for example, may be less important at a division or entity level. At higher levels of the entity, risks are likely to have a greater impact on reputation, brand, and trustworthiness.

Using standardized risk terminology and categories helps in the assessment of risks at all levels of the organization. Common risks across business units, divisions, and functions can also be grouped. For example, the risk of technology disruptions identified by multiple divisions may be grouped and assessed collectively. Similarly, the risks measured at escalating 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 business units or divisions.

Figure 8.5 illustrates the risk inventory mapped to strategy and business objectives. In a "top-down" entity-level risk assessment, risk 4 may be assessed to have a low level of severity. In a business unit–level assessment, risk 4 may be considered more significant and therefore have a greater severity.

In order for risk assessment practices to be complete, a top-down assessment considers those risks identified and assessed at lower levels. For example, an entity-level assessment would assess entity-level risks, but should also consider those severe risks identified at the entity business objective level, such as risk 2, to determine if, given their severity, they are an entity-level concern.

Figure 8.5: Assessing Risk at Different Levels

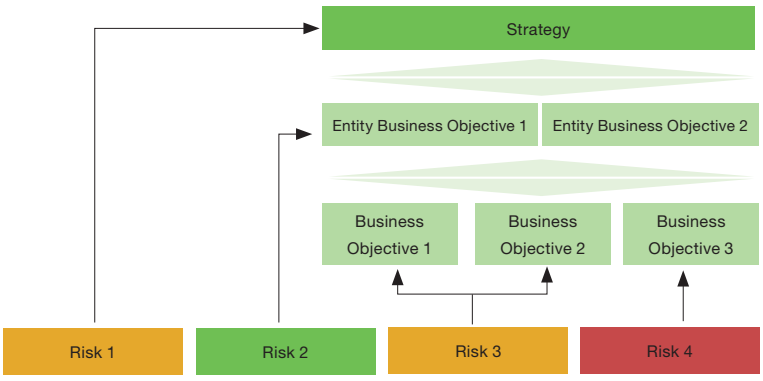
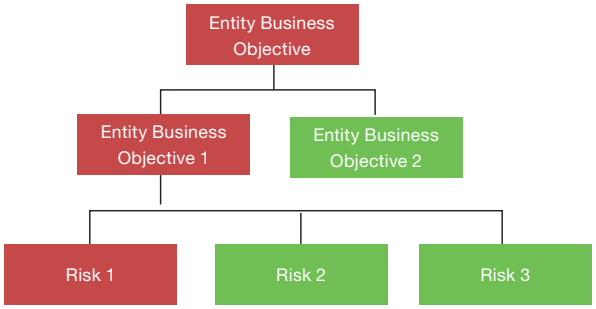


Figure 8.6 illustrates four common scenarios.

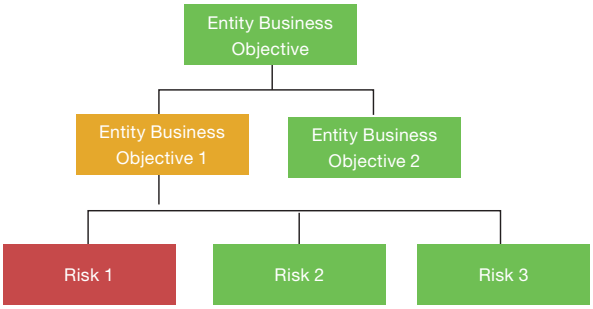
- In scenario 1, the organization recognizes that the risk could impact the business objective as well as the entity-level business objective. For example, a safety error in a manufacturing process can, given its magnitude, impact the entity as whole.
- In scenario 2, a risk diminishes in severity at higher levels of the entity, indicating that it does not pose the same potential impact to the entity as a whole. For example, a backlog in transactions may pose a risk to the operating unit managing processing but may not have a significant impact on the business objective overall, and at the entity level may have little to no impact. However, if the backlog grows, this risk could elevate to scenario 3 or even scenario 1.
- In scenario 3, two risks individually have moderate severity assessments, but together they impact the business objectives and entity more significantly, and therefore they are assessed as more severe. For example, the inability to recruit employees for common support functions such as legal expertise represents a low risk to each operating unit but starts to impact the entity more significantly at a business objective level as the trend could have a detrimental impact on the ability to achieve a business objective heavily dependent on legal expertise. Yet, at an entity level, that risk may not be as significant given the importance of the business objective to the strategy.
- In scenario 4, certain risks impact the entire entity. For example, the risk of a takeover bid by competitors impacts the strategy of the entity as a whole, but may not impact business-level objectives individually.

Figure 8.6: Assessing Severity at Different Levels

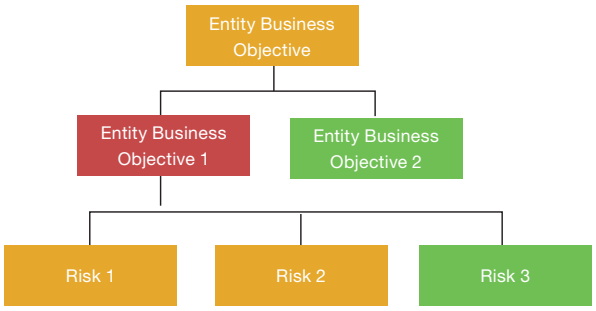
1) Business objective–level risk retains severity at higher levels



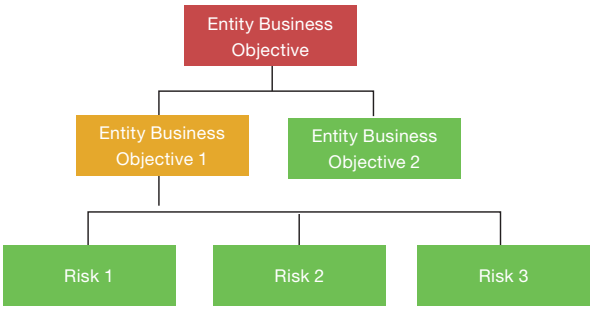
2) Business objective–level risk decreases in severity at higher levels



3) Business objective–level risk increases in severity at higher levels



4) Entity business objective–level risk decreases in severity at lower levels



Selecting Severity Measures

Management selects measures to assess the severity of risk. Generally, these measures align to the size, nature, and complexity of the entity and its risk appetite. Different thresholds 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 are tailored to the level of assessment—by entity or operational unit. Acceptable amounts of risk to financial performance, for example, may be greater at an entity level than an operating unit level.

Management determines the relative severity of various risks in order to select an appropriate risk response, allocate resources, and support management decision-making and performance. Measures may include:[23]

- *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.
- *Likelihood:* The possibility of a risk occurring. This may be expressed in terms of a probability or frequency occurring. Likelihood may be expressed in a variety of ways, as the following examples show:
    - **Qualitative:** "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., twelve months] is remote."
    - **Quantitative:** "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., twelve months] is 80%."
    - **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., twelve months] is once every twelve months."

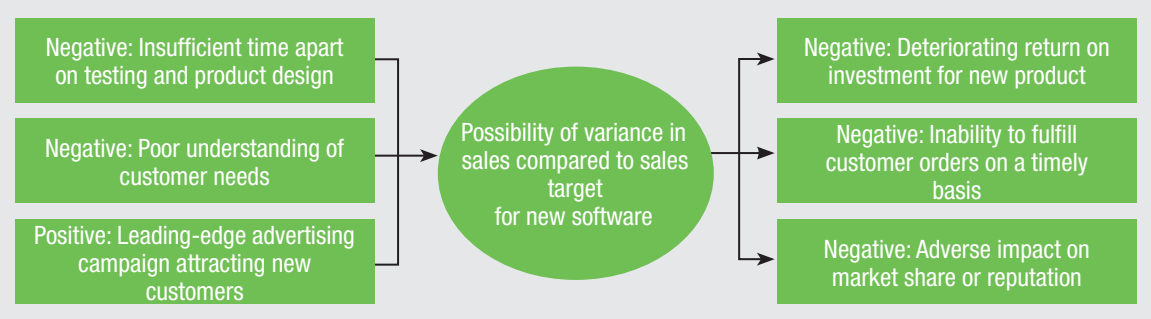
As part of the assessment process, management considers potential combinations of likelihood and impact. For example, there may be a low risk of operational incidents resulting in losses greater than 20% of the entity's revenue. At the same time, there may be a higher likelihood of operational incidents resulting in losses of less than 1% of the entity's revenue. Whenever management identifies when a risk would be disruptive or necessitates a change in risk response, that risk is accounted for in the assessment activities.

The time horizon used to assess risks should be the same as that used for the related strategy and business objectives. For instance, if the business objectives focus on a three-year time horizon, management would consider risks within that time frame. 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. However, when assessing risks of the mission, vision, or strategy, the time frame may be longer. Management needs to be cognizant of the longer time frames and not ignore risks that might emerge or occur further out.

Additionally, risk emanates from multiple sources and results in different impacts. Root causes can have a positive or negative impact on assessment of a risk. Figure 8.7 illustrates the variety of results that may occur from a variety of sources.

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

Figure 8.7: Root Causes and Impacts of Risk



Severity measures should align with the strategy and business objectives. Example 8.2 illustrates how an organization identifies the risks to its business objectives and applies appropriate measures. When different impacts are identified for a business objective, management provides guidance on how to assess the severity of the impact. 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.

Assessment Approaches

Risk assessment approaches may be qualitative, quantitative, or a combination of both.

- Qualitative assessment approaches, such as interviews, workshops, surveys, and benchmarking, are often used when it is neither practicable nor cost-effective to obtain sufficient data for quantification. Qualitative assessments are more efficient to complete; however, there are limitations in the ability to identify correlations or perform a cost-benefit analysis.
- Quantitative assessment approaches, such as modeling, decision trees, Monte Carlo simulations, etc., allow for increased granularity and precision, and support a cost-benefit analysis. Consequently, quantitative approaches are typically used in more complex and sophisticated activities to supplement qualitative techniques. Quantitative approaches include:
    - Probabilistic models (e.g., value at risk, cash flow at risk, operational loss distributions) that associate a range of events and the resulting impact with the likelihood of those events based on certain assumptions. Understanding how each risk factor could vary and impact cash flow, for example, allows management to better measure and manage the risk.
    - Non-probabilistic models (e.g., sensitivity analysis, scenario analysis) use subjective assumptions to estimate the impact of events without quantifying an associated likelihood on a business objective. For example, scenario analysis allows management to understand the impact on a business objective to increase profitability under different scenarios, such as a competitor releasing a new product, a disruption in the supply chain, or an increase in product costs.

Depending on how complex and mature the entity is, management may rely on a degree of judgment and expertise when conducting the modeling. Regardless of the approach used, any assumptions should be clearly stated.

Example 8.2: Aligning Business Objectives, Risk, and Severity Measures

Objective Type	Business Objective	Identified Risk	Target and Tolerance	Severity Measures	
				Rating/ Impact Type	Likelihood (Probability)
Business objectives for Snacks (operating unit)	Continue to develop innovative products that interest and excite consumers	The possibility that the organization fails to develop new products that exceed customer expectations	Target: 8 products in development at all times Tolerance: Number of new products in development to be between 6 and 12 at all times	Moderate impact to consumer satisfaction	Possible
Business objectives for Human Resources	Recruit and train product sales managers in the coming year	The possibility that the organization is unable to identify appropriately qualified people for sales managers	Target: Recruit 50 product sales managers Tolerance: The entity recruits between 35 and 50 product managers in the coming year	Minor impact to operational/Human Resources	Possible
		The possibility that the organization is unable to schedule training for new sales managers	Target: Train 95% of sales managers Tolerance: The entity trains a minimum of 85% of product sales managers in the coming year		Unlikely

The anticipated severity of a risk may influence the type of approach used. 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 (e.g., stress testing). Conversely, high-frequency, low-impact risks may be more suited to data tracking and cognitive computing. To reach consensus on the severity of risk, organizations may employ the same approach they used as part of the risk identification.

Assessments may also be performed across the entity by different teams. In this case, the organization establishes an approach 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.

Finally, part of risk assessment is seeking to understand the interdependencies that may exist

between risks. Interdependencies can occur where multiple risks impact 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 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.

Inherent, Target, and Residual Risk

As part of the risk assessment, management considers inherent risk, target residual risk, and actual residual risk.

- *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 to alter the severity of the risk.
- *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. Where actual residual risk exceeds target risk, additional actions should be identified that allow management to alter risk severity further.

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.

Depicting Assessment Results

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. Each risk plotted on the heat map assumes a given level of performance for that strategy or business objective.

Assessed risks for a given business objective are plotted on the heat map using the severity measures selected by the entity for a given level of performance. The various combinations of likelihood and impact (severity measures), given the risk appetite, are color coded to reflect a particular level of severity. In Figure 8.8, the entity has four risk severity ratings ranging from red to green. The color coding aligns to a particular severity outcome and reflects the risk appetite of the entity. Risk-averse entities may code more squares in red compared to risk-aggressive entities.

Figure 8.8: Business Objective Heat Map

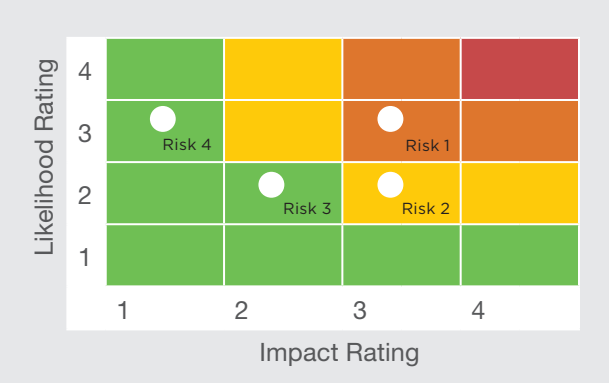


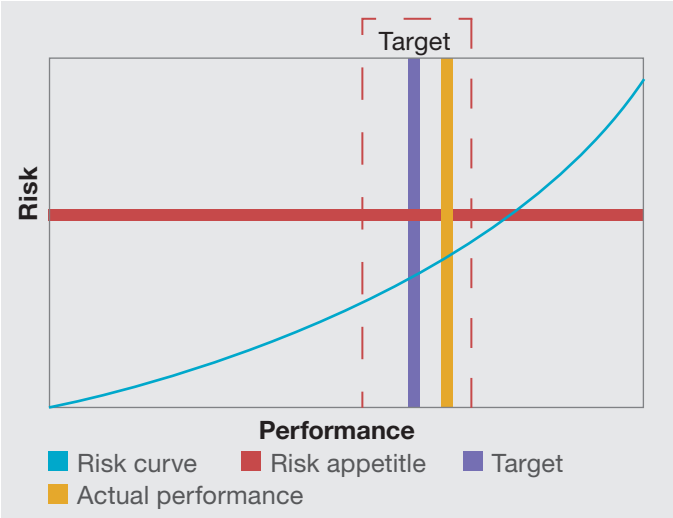
Figure 8.9 illustrates the risk profile for a single business objective and a given level of performance. Should the level of performance change, the corresponding changes in each of the risks are captured. This may result in new risks, risks shifting in severity, or risks being removed.

It is the risk inventory that forms the basis from which an organization is able to construct a risk profile (as shown in Figure 8.9). Each data point on the risk curve represents the combination and severity of risks for that business objective (as illustrated in a disaggregated manner using the heat map in Figure 8.8). Management may use the risk profile in its assessment to:

- Confirm that performance is within the tolerance.

- 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 may impact its performance or the achievement of its strategy and business objectives.

Figure 8.9: Business Objective Risk Profile



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 poor sales due to not stocking a diverse product range that will appeal to a broad group of customers. Management is also aware that changes in marketing and advertising efforts can significantly affect sales. Focusing on the business objective of sales, management is able to better understand the risks that have an impact on sales. Understanding the severity of different risks to the same business objective, management can make risk-aware decisions about the diversity of products in stock and the desired budget to spend on marketing and advertising costs in order to manage the risk of low sales.

Identifying Triggers for Reassessment

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, and they serve as early-warning indicators of changes to assumptions underpinning the severity assessment. A trigger may be 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. Triggers may also come from a competitor (e.g., competitor's product recalled for defects).

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

Management should identify and mitigate the effect of bias in carrying out risk assessment practices. For example, confidence bias may support a pre-existing perception of a known risk. Additionally, how a risk is framed can also affect how risks are interpreted and assessed. For example, for a given risk, there may be a range of potential impacts, each with a separate likelihood. Thus, a risk with a low likelihood but high impact could have the same outcome as a high likelihood, low impact; however, one risk may be acceptable to the organization while the other is not. As such, the manner in which the risk is presented and framed to management is critical to mitigate any bias.

Bias may result in the severity of a risk being under- or overestimated, and limit how effective the selected risk response will be. Underestimating the severity may result in an inadequate response, leaving the entity exposed and potentially outside of the entity's risk appetite. Overestimating the severity of a risk may result in resources being unnecessarily deployed in response, creating inefficiencies in the entity. Additionally, it may hamper the performance of the entity or affect its ability to identify new opportunities.

Principle 12: Prioritizes Risks

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

Establishing the Criteria

Organizations prioritize risks in order to inform decision-making on risk responses and optimize the allocation of resources. Given the resources available to an entity, management must evaluate the trade-offs between allocating resources to mitigate one risk compared to another. The prioritization of risks, given their severity, the importance of the corresponding business objective, and the entity's risk appetite helps management in its decision-making.

Priorities are determined by applying agreed-upon criteria.[24] 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 and the impact on business objectives relating to product innovation).
- *Complexity:* The scope and nature of a risk to the entity's success. The interdependency of risks will typically increase their complexity (e.g., risks of product obsolescence and low sales to a company's objective of being market leader in technology and customer satisfaction).
- *Velocity:* The speed at which a risk impacts an entity. The velocity may move the entity away from the acceptable variation in performance. (e.g., the risk of disruptions due to strikes by port and customs officers affecting the objective relating to efficient supply chain management).
- *Persistence:* How long a risk impacts an entity (e.g., the persistence of adverse media coverage and impact on sales objectives following the identification of potential brake failures and subsequent global car recalls).
- *Recovery:* The capacity of an entity to return to tolerance (e.g., continuing to function after a severe flood or other natural disaster). Recovery excludes the time taken to return to tolerance, which is considered part of persistence, not recovery.

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

Prioritizing Risk

Risks with similar assessments of severity may be prioritized differently. That is, two risks may both be assessed as "medium," but management may give one more priority because it has greater velocity and persistence (see Example 8.3), or because the risk response for one risk provides a higher risk-adjusted return than for other risks of similar severity.

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

Example 8.3: Prioritizing Risk

For a large restaurant chain, responding to the risk that customer complaints remain unresolved and attract adverse attention in social media is considered a greater priority than responding to the risk of protracted contract negotiations with vendors and suppliers. 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.

24 The criteria may also be used as a consideration when assessing the severity of a risk as discussed in Principle 11.

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

Management should also compare risk appetite when prioritizing risks. Risks that result in the entity approaching the risk appetite for a specific business objective are typically given higher priority (see Example 8.4). Additionally, performance levels that approach the outer bounds of tolerance may be given priority.

Through 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.

Example 8.4: Relationship of Risk Profile to Risk Appetite

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 less likely to achieve its business objectives of providing reliable service. 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.

Prioritization at All Levels

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 evaluated as 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.

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 category, which enables common risks to be prioritized consistently across the entity. The result is a more consistent and efficient risk response than would have occurred if each risk had been prioritized separately.

Risk owners are responsible for using the assigned priority to select and apply appropriate risk responses in the context of business objectives and performance targets. 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.

Bias in Prioritization

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.

Principle 13: Implements Risk Responses

The organization identifies and selects risk responses.

Choosing Risk Responses

For all risks identified, management selects and deploys a risk response. Management considers the severity and prioritization of the risk as well as the business context and associated business objectives. Finally, the risk response also accounts for the performance targets of the organization. Risk responses fall within the following categories:

- *Accept:* No action is taken to change the severity of the risk. This response is appropriate when the risk to strategy and business objectives is already within risk appetite. 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 risk to an acceptable level of severity.
- *Pursue:* Action is taken that accepts increased risk to achieve improved performance. This may involve adopting more aggressive growth strategies, expanding operations, or developing new products and services. When choosing to pursue risk, management understands the nature and extent of any changes required to achieve desired performance while not exceeding the boundaries of acceptable tolerance.
- *Reduce:* Action is taken to reduce the severity of the risk. This involves any of myriad everyday business decisions that reduces 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.

These categories of risk responses require that the risk be managed within the business context, business objectives, performance targets, and organization's risk appetite. 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 tolerance. 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.

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 risk associated with the expedited approval of a new product in favor of the opportunity 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

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 structure, 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.
- *Prioritization of risk:* The priority assigned to the risk informs the allocation of resources. Risk 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 priority.
- *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 a range of tolerance.
- *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.

Often, any one of several risk responses will bring the residual risk in line with the tolerance, 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.

The risk response may change the risk profile (see Example 8.5). Once management selects a risk response, control activities[25] are necessary to ensure that those risk responses are carried out 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.

Example 8.5: Changing Risk Profiles

A midsized fruit farmer considers purchasing weather-related insurance for floods or storms that would offset any decline in production below a certain minimum volume. The resulting risk profile for production levels would account for the potential performance outcomes covered by insurance.

Considering Costs and Benefits of Risk Responses

Management must consider the potential costs and benefits of different risk responses. Generally, anticipated costs and benefits are commensurate with the severity and prioritization of the risk. For example, a high-priority risk with a greater severity may warrant increased resource costs, given the anticipated benefits of the response.

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

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

organization can either select a response or choose to revisit the entity's strategy and business objectives.

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: Relationship of Risk Profile to Risk Appetite

An 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 to achieve its objectives relating to regulatory compliance.

Additional Considerations

Selecting one risk response may introduce new risks that have not been previously identified or may have unintended consequences. For example, for the fruit farmer in Example 8.5, the risk of floods damaging the crops was reduced by purchasing insurance; however, the farmer may now be at risk of low cash flow.

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 will likely provide only marginal changes to the severity of a risk. Management channels any new opportunities back to strategy-setting.

Principle 14: Develops Portfolio View

The organization develops and evaluates a portfolio view of risk.

Understanding a Portfolio View

Enterprise risk management allows 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 tolerance.

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 could disrupt the entity as a whole.

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 be well within the range in another. For example, some operating units have higher risk than others, yet the overall risk remains 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 value.

Developing a Portfolio View

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 (other qualitative methods can also be used to develop this portfolio view).

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. The portfolio view in Figure 8.10 illustrates the alignment of risks to business objectives and the relationship between different objectives.

In developing a view of risk, there are four levels in order of ascending level of integration (from minimal to maximum):

- *Minimal Integration—Risk View:* At the risk-centric view, the entity identifies and assesses discreet risks. The predominant focus is on the underlying risk event rather than the objective; for example, the risk of a breach impacting compliance of the entity with local regulations.
- *Limited Integration—Risk Category View:* This view uses information captured in the risk inventory view and organizes risks using categories or another classification scheme. Risk categories often reflect the entity's operating structure and inform roles and responsibilities. A compliance department, for example, will have responsibilities for helping the organization manage its compliance-related risks.

- *Partial Integration—Risk Profile View:* Adopting a more integrated view, an organization focuses on business objectives and the risks that align with those objectives (e.g., all objectives potentially impacted by compliance-related risks). Further, dependencies that may exist between business objectives are identified and considered. For example, an objective of enhancing operational excellence may be a prerequisite for strengthening the balance sheet and growing market share. This view relies on information used to create the risk-centric or risk-category view.
- *Full Integration—Portfolio View:* At this level, the focus shifts to the overall entity strategy and business objectives. Greater integration supports identifying, assessing, responding to, and reviewing risk at the appropriate levels for decision-making. Boards and management focus greater attention on the achievement of strategy while responsibility and management of business objectives and individual risks within the risk inventory cascade throughout the entity. Using the same example, the board reviews and challenges management on how the entity is enhancing its operational excellence including the management of compliance-related risks.

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.
- Demonstrate a positive or negative correlation to changes occurring in the severity of other risks.

Figure 8.10 Portfolio View of Risk

Using Figure 8.10 as an example, an organization develops its portfolio view and observes the following characteristics:

- *Severity of technology disruptions* increases as risks are progressively aggregated, recognizing the reliance that multiple businesses have on common operating systems and technology.
- *Risk of counterparty defaults* decrease in severity as the entity does not have a single creditor considered large enough to impact the entity as a whole.
- *Risk of low sales from multiple operating units* may act as a natural hedge where low sales in one operating unit are offset by strong sales in another.
- *Risk of currency fluctuations* may also act as a natural hedge where currency changes in one country offset changes in another.
- *Strong positive correlation between risk of product recalls and the risk of compliance breaches* increases the priority of risk responses to both risks.
- *Strong positive correlation between the business objectives* requires investing in best-in-class technology solutions and minimizes losses and inefficiencies that are taken into account when selecting associated risk responses.

Developing a portfolio view of the risks to the entity enables risk-based decision-making and helps set performance targets and manage changes in either the performance or the risk profile. Important considerations in setting targets and responding to change include understanding which risks are likely to increase or decrease, whether new risks are introduced, and whether existing ones become less relevant. By using a portfolio view to understand the relationship between risk and performance, the organization can assess the results of the strategy and business objectives in accordance with the entity's risk appetite.

Analyzing the Portfolio View

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.

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.

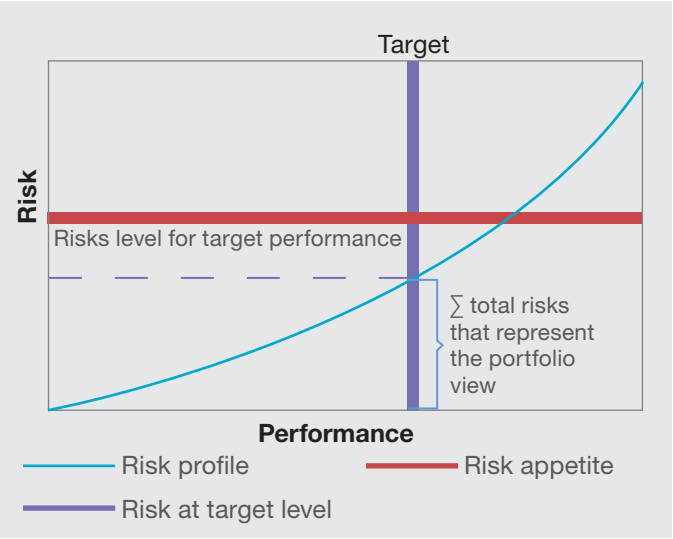
Undertaking stress testing, scenario analysis, or other analytical exercises helps an organization to avoid or better respond to big surprises and losses. The organization uses different techniques to assess the effect of changes in the business context or other variables on a business objective or strategy. 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 affect 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.

Stress testing helps an organization understand how the shape or height of the risk curve may respond to potential changes. For example:

- Validation of events that could become disruptive and cause the risk curve to exceed risk appetite (e.g., the magnitude of a potential funding gap that impacts the viability of the business, which would be represented by the intersect of the risk curve with the risk appetite of the entity.
- The extent to which the risk curve may shift up or down in response to a change (e.g., confirming to what extent changing economic health indicators such as unemployment levels and gross domestic product represent a sufficient deterioration in the business context and causing the risk curve to shift up).
- Risk responses that can cause sections of the curve to become flatter (e.g., diversifying products entering into new financial hedging strategies or purchasing additional insurance).
- The ease at which the organization can move along the curve. The speed and agility of the organization to make decisions and travel along the risk curve to a new desired intersection of risk and performance (e.g., the ability and speed of adjusting production volumes in response to changes in sales).

These practices help to assess the adaptive capacity of the entity. They 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. Figure 8.11 illustrates a portfolio view of risk.

Figure 8.11: Risk Profile Showing Risk as a Portfolio View



9. Review and Revision

Principles Relating to Review and Revision

15. **Assesses Substantial Change:**
    The organization identifies and assesses changes that may substantially effect strategy and business objectives.
16. **Reviews Risk and Performance:**
    The organization reviews entity performance results and considers risk.
17. **Pursues Improvement in Enterprise Risk Management:**
    The organization pursues improvement of enterprise risk management.

Introduction

An entity's strategy or business objectives and enterprise risk management practices and capabilities may change over time as the entity adapts to shifting business context. In addition, the business context in which the entity operates can also change, resulting in current practices no longer applying or sufficient to support the achievement of current or updated business objectives. As necessary, the organization revises its practices or supplements it capabilities.

Principle 15: Assesses Substantial Change

The organization identifies and assesses changes that may substantially affect strategy and business objectives.

Integrating Reviews into Business Practices

Organizations typically anticipate many changes within setting of strategy and business objectives and performance, but they need to also be aware of the potential for larger, substantial changes that may occur and have a more pronounced effect. Substantial change may lead to new or changed risks, and affect key assumptions underpinning strategy. Practices for identifying such changes should be built into business activities 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.

Substantial changes such as acquiring an entity or implementing a new system could potentially change the entity's portfolio view of risk or affect how enterprise risk management functions. In the case of an acquisition, integrating the acquired company's operations could affect 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.

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 in both the internal and external environment are highlighted below.

Internal Environment

- *Rapid growth:* When operations expand quickly, existing structures, business activities, 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.
- *Innovation:* Whenever innovation 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. Innovation 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 may have a different philosophy, or may focus solely on performance to the exclusion of risk appetite or tolerance.

External Environment

- *Changing regulatory or economic environment:* Changes to regulations or in the economy 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 public companies. The revelation of patients being treated poorly in one care facility may prompt additional 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.

Identifying substantial changes, evaluating their effects, 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 16: Reviews Risk and Performance

The organization reviews entity performance and considers risk.

Integrating Reviews into Business Practices

Much of the focus on enterprise risk management is on managing risk—either reducing the type and amount of risk to acceptable levels or appropriately pursing new opportunities as they emerge. Over time, an entity may not conduct its practices as efficiently as intended, thereby causing risk to manifest and affect performance. From time to time, the organization may wish to consider its enterprise risk management capabilities and practices. Observations may relate to incorrect assumptions, implemented practices, entity capabilities, or cultural factors. Sometimes, however, performance is affected because of the inherent nature of risk, which an organization cannot predict with complete accuracy. By reviewing performance, organizations seek answers to questions such as:

- **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. This may involve using measures relating to objectives or other key metrics. 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?** Reviewing performance confirms whether risks were previously identified, or whether new, emerging risks have occurred. The organization also reviews whether the actual risk levels are within the boundaries established for tolerance. For example, reviewing performance helps confirm that the risk of delays due to additional permit requirements for construction did occur and affected the number of new offices opened, and whether the number of offices to be opened is still within the range of acceptable performance.
- **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 (e.g., more problems, delays, and unexpected events than initially assessed).

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 objectives:* 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.
- *Review culture:* An organization may wish to review its culture and determine whether it is embracing the actions in a risk-aware manner. Is the organization comfortable taking enough risk to succeed, or is it prone to taking too much risk and incurring adverse outcomes?
- *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.
- *Reassess severity of risk results:* An organization may re-do 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 decide 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. As part of reviewing risk responses, the organization may also consider monitoring activities developed and implemented as part of internal control.[26]
- *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.

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.

Where reviewing performance repeatedly identifies new risks that were not identified through the organization's risk identification practices, 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 practices can be found in Principle 17.

26 Additional information on monitoring activities is discussed in *Internal Control–Integrated Framework*.

Considering Entity Capabilities

Part of reviewing 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.

Corrective action may include reallocating resources, revising business objectives, or exploring alternative strategies (see Example 9.1).

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 tolerance occur, or where performance represents a disruption to the achievement of the entity's strategy, the organization may revise its strategy.

Example 9.1: Considering Entity Capabilities

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 have 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) provides the city with enough revenue to support its annual operating budget and fund other programs. However, an occupancy rate greater than 85% increases risks relating to the usage of the public transportation system, demands for peace officer presence, and stresses on natural resources. The city tracks patterns in its tourism industry to make more risk-aware decisions on the aggressiveness of its future marketing campaigns and actively managing risk influenced by tourism.

Principle 17: Pursues Improvement in Enterprise Risk Management

The organization pursues improvement of enterprise risk management.

Pursuing Improvement

Even those entities with suitable enterprise risk management can become more efficient. By embedding continual evaluations into business practices, organizations can systematically identify potential improvements to their enterprise risk management practices. Separate evaluations may also be helpful.[27] Pursuing improved enterprise risk management should occur throughout the entity (see Example 9.2).

Example 9.2: Continual Improvement

A government agency learns that it has stronger practices in place for establishing and implementing governance capabilities and for instilling the desired culture. Conversely, the organization's practices for establishing and implementing information and communications capabilities present opportunities for improvement. While management monitors improvement opportunities for all enterprise risk management components, it concentrates on developing its information and communications practices.

Management pursues continual improvement throughout the entity (functions, operating units, divisions) 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:* Reviewing performance 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 practices to reduce the number of shortcomings and enhance enterprise risk management.
- *Organizational change:* By pursuing continual improvement, an organization can identify the need for organizational changes such as a change in the governance structure. 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:* Reviewing performance 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 performing well and is less volatile than originally thought, the organization can respond by increasing its risk appetite for similar future initiatives.
- *Risk categories:* An organization that continually pursues improvement can identify patterns as the business changes, which can lead the entity to revise its risk categories. For example, one

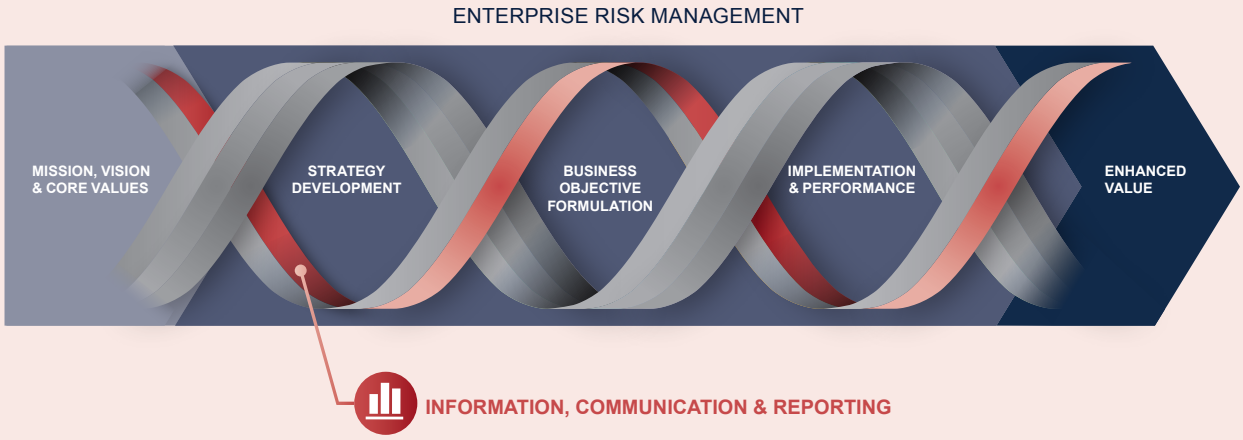
27 Readers may also wish to review the discussion on monitoring activities in *Internal Control–Integrated Framework*.

entity's risk categories does not include cyber risk, but now that the entity has decided to offer several on-line products and services, it is revising the categories to include cyber risk so it can accurately map its strategy.

- *Communications:* Reviewing performance can identify outdated or poorly functioning communication processes. For example, in reviewing 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:* Reviewing 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.

10. Information, Communication, and Reporting

Principles Relating to Information, Communication, and Reporting



18. **Leverages Information and Technology:**
    The organization leverages the entity's information systems to support enterprise risk management.
19. **Communicates Risk Information:**
    The organization uses communication channels to support enterprise risk management.
20. **Reports on Risk, Culture, and Performance:**
    The organization reports on risk, culture, and performance at multiple levels and across the entity.

Introduction

Advances in technology and business have resulted in exponential growth in volume of, and attention on, data. Organizations today are challenged by the enormous quantity of data and the speed at which it all must be processed, organized, and stored. With so much data available, organizations may be feeling weighed down by "information overload." In this environment, it is important that organizations provide the right information, in the right form, at the right level of detail, to the right people, at the right time.

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. Organizations can also structure data and information into consistent categories. In this way, they can identify risks that could affect the entity's strategy and business objectives.

Principle 18: Leverages Information and Technology

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

Putting Relevant Information to Use

Organizations leverage relevant information when they apply enterprise risk management practices. "Relevant information" is simply information that helps organizations be more agile in their decision-making, giving them a competitive advantage. Organizations use information to anticipate situations that may get in the way of achieving strategy and business objectives. Risk information is more than a repository of historical risk data. It needs to support an understanding and development of a complete current and evolving risk profile.

Organizations consider what information is available to management, what information systems and technology are in use for capturing that information (which may be more than is needed), and what the costs are of obtaining that information. Management and other personnel can then identify how information supports the enterprise risk management practices, which may include any of the following:

- For governance and culture-related practices, the organization may need information on the standards of conduct and individual performance in relation 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 management gathers information by testing the staff's knowledge to determine whether they understand what is expected of them.
- For strategy and objective-setting related practices, the organization 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. All of these provide relevant information on the types and amount of risk an entity may be willing to accept and strategy it pursues.
- For performance-related practices, organizations may need information on their competitors to assess changes in the amount of risk. For example, a large residential real estate company may assess the risk of losing market share to smaller boutique firms. The information they need is their competitors' commission pricing models and on-line marketing plans. If their competitors' commission rates are low and aggressive, and their on-line presence is widespread, the large company may review its ability to achieve its sales targets.
- For review and revision-related practices, organizations may need information on emerging trends in enterprise risk management. Organizations can collect such information from attending enterprise risk management conferences and following industry-specific blogs.

Today data is generated so fast that it is often a challenge for management to process and refine it into usable information. Information systems can help entities meet this challenge. However, the focus should not be on creating a new and separate information system or even separate streams for enterprise risk management. It is usually more efficient for an organization to leverage its existing information systems to capture what it needs to understand risk, to make risk-aware decisions, and to fulfill reporting requirements.

To be useful, information must be available to decision-makers when it is needed. It is also essential that the information be of high quality. If the underlying data is inaccurate or incomplete, management may not be able to make sound judgments, estimates, or decisions.[28] To maintain high-quality information, organizations implement data management systems and establish information management policies with clear lines of responsibility and accountability.

Evolving Information

Data transformed into information may come from both structured and unstructured sources. Structured data generally refers to information that is highly organized and readily searchable (e.g., database files, public indexes, or spreadsheets). In contrast, unstructured data does not follow a predefined data pattern, nor is it organized (e.g., email messages, photos, videos, word processing documents). Several research studies have estimated that today unstructured data outweighs structured data by more than 80%.

Data analytics have historically relied on predefined patterns when converting data to information. Now, advances in cognitive computing, such as artificial intelligence,[29] data mining, and machine learning can collect, convert, and analyze large volumes of unstructured data into information that helps organizations to make better business decisions. These advances, combined with human analysis, allow management greater insight. Example 10.1 illustrates the application of unstructured information.

Example 10.1: Using Unstructured Information in Decision-making

A consumer retailer uses artificial intelligence to attain better information on improving the customer experience. In this way, management is able to gather insights about consumers through social media, such as purchasing behavior, including historical patterns and preferences. The insights can be used to reduce the risk of over- or understocking inventory, as they provide management with a better view of the right inventory levels. This improved inventory management reduces operational and resource costs and enhances the customer experience.

Example 10.2: Determining Information Requirements

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 rely on various data such as demographics of the testing population, number of side effects, duration of studies, and type of application. Data is captured from internal patient feedback and through monitoring social media conversations.

In short, advances in data analytics can help organizations avoid "information overload" and use the huge amount of data now available to its advantage. They may be able to detect correlations in business performance that are not readily apparent with a more traditional approach to data analysis. Or they may be able to identify likely trends in performance earlier. They may even be able to more thoroughly evaluate key assumptions embedded into a strategy, which in turn provides added insight in decisions on alternative strategies, business objectives, and setting of performance targets. Having more information pertinent to decision-making also reduces reliance on individual experience and judgment in making those decisions.

28 Further discussion on information quality is available in *Internal Control–Integrated Framework*, specifically Principle 13.

29 Artificial intelligence can be defined as theory and development of computer systems that perform tasks that normally require human intelligence such as speech recognition, decision-making, visual perception, and other factors.

Data Sources

Data that is transformed into information becomes knowledge (e.g., analysis of comments posted on social media identifies potential risks to the entity's brand). Therefore, data requirements should be based on information requirements. Example 10.2 illustrates how a company determines that it requires data in order to provide compliance information to an external stakeholder.

Data can be collected from a variety of sources and in a variety of forms. Figure 10.1 lists examples of structured and unstructured data.

Figure 10.1: Internal Data Sources

Sources	Examples of Data	Structured	Unstructured
Board and management meetings	Meeting minutes and notes on potential transactions		✓
Customer satisfaction survey	Feedback from priority customers about employee interactions	✓	✓
Due diligence activities	Staffing increases and decreases due to restructuring agreements	✓	
Email	Information relating to decision-making and entity performance		✓
Government-produced geopolitical reports and studies	Population changes in emerging markets	✓	
Manufacturer reports	Emerging interest in products shipped from a competing manufacturer		✓
Marketing reports from website tracking services	Number of website visits, duration on a page, and conversions into customer purchases	✓	
Metadata	Details on video file content, including technical details and text descriptions of scenes	✓	✓
Public indexes	Data from water scarcity index for beverage manufacturer or agriculture company considering new locations	✓	
Social media and blogs	Feedback and count of negative and positive comments on a company's new product	✓	✓

Categorizing Risk Information

Organizations can classify the information they capture by using common risk categories.[30] These categories may be organized by functional areas, such as internal audit, information management, or operational risk management. They may also be based on the size, scale, and complexity of the entity.

Using a common set of categories helps organizations aggregate risk information to determine if there are any potential impacts from concentrations of risk across the entity. Such a structure of categories also helps them assess risks that could affect the entity's strategy and business objectives. It also serves as the basis for developing consistent enterprise risk responses and reporting.

30 Some organizations refer to these common risk categories as a "risk taxonomy."

Managing Data

Data must be well managed to provide the right information to support risk-aware decisions. That requires capturing and preserving the quality of the data while allowing different technologies to exchange and use it. Effective data management considers three key elements: data and information governance, processes and controls, and architecture.

- *Data and information governance* help to deliver standardized, high-quality data to end users in a timely, verifiable, and secure manner. They also help to standardize data architecture, authorize standards, assign accountability, and maintain quality. As well, they define clear roles and responsibilities for data owners and risk information owners.
- *Processes and controls* help an entity reinforce the reliability of data and allow for corrections to be made as needed. For example, organizations may have a process to identify instances and patterns of both low- and high-quality data, and whether that data is relevant to meeting requirements. Or they may be able to identify data consistency, redundancy, availability, and accuracy. 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.
- *Data management architecture* refers to the fundamental design of the technology. 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.

Using Technology to Support Information

Technology is often associated with information systems. Yet, technology often involves more than processing and reporting of data; it also can help the organization to carry out activities. Robotics used in manufacturing, smart appliances that manage energy use in residential and commercial buildings, and wearable technology are all examples of how technology can help an organization manage specific risks. Example 10.3 illustrates how technology is helping to both manage the risk and capture information that aids in decision-making.

However, technology can also introduce new risks to an entity, which 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 against the costs of selecting or developing supporting technologies.

Example 10.3: Information Systems

A healthcare organization has been challenged to find ways to reduce the incidents of seniors missing doses of prescription medicines. Missing prescribed dosages can reduce the benefits of the drugs and increase health risks to the patient. In response, the company has distributed wearable technology to patients that identifies cases of them missing a dose and tracks the general health of each patient. This information is reported to the healthcare provider.

Changing Requirements

Management leverages and designs its technology 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 technologies. For instance, shifting customer expectations may require organizations to change their technology to allow for more timely information gathering and more active reviewing of comments on social media.

Principle 19: Communicates Risk Information

The organization uses communication channels to support enterprise risk management.

Communicating with Stakeholders

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.

Internally, management communicates the entity's strategy and business objectives clearly throughout the organization 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 tolerance.
- 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.

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.

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, hotlines, or other channels.

Communicating with the Board

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 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 10.4).

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, cost 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.

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.

Example 10.4: Communicating with the Board

A company aiming to improve risk communication chose to revise its 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.

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.
- Capture instances where current performance levels are approaching the tolerance of acceptable variation in performance and the plans in place to manage performance.
- Provide a longitudinal perspective of risk exposures including historical data, explanations of trends, and forward-looking information 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.

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 defined response for that risk either planned or in place. 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 management to provide more timely and insightful dialogue, rather than waiting for these risks to evolve within the entity.

Methods of Communicating

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 stating expectations for enterprise risk management in employee performance goals and subsequent periodic performance evaluations.

Communication 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.

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 indexes).
- *Informal/verbal communications* (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).

In addition to the list 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 20: Reports on Risk, Culture, and Performance

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

Identifying Report Users and Their Roles

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.
- External stakeholders (regulators, rating agencies, community groups, and others).
- Other parties that require reporting of risk in order to fulfill their roles and responsibilities.

It is also important to understand the governance and operating structures 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.

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 to senior management present a more granular level and support decisions on strategic-setting 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.

Risk reporting may be done by any team within the operating structure. Teams prepare reports, disclosing information in accordance with their risk management responsibilities. For example, teams may 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

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

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 the entity operates, can help management connect historical information to 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

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 risks 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 effect on strategy and business objectives.
- *Analysis of new, emerging, and changing risks* provides the forward-looking view to anticipate changes to the risk inventory, effects on resource requirements and allocation, and the anticipated performance of the entity.
- *Key performance indicators and measures* outline the tolerance 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.

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

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.

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 impact of potential risk in meeting those objectives.

Reporting on Culture

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

Key indicators are used to predict a risk manifesting. They are usually quantitative, but can be qualitative. Key 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 indicators support a proactive approach to performance management (see Example 10.5).

Key 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 such as supplier delays, labor shortages, or equipment downtime.

Example 10.5: Using Key Indicators

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 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.

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

Reporting Frequency and Quality

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.

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 suitability 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.

Glossary of Key Terms

- **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.
- **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.
- **Enterprise Risk Management:** The culture, capabilities, and practices, integrated with strategy-setting and its performance, that organizations rely on to manage risk in creating, preserving, and realizing value.
- **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 structure.
- **External Environment:** Anything outside of the entity that influences the ability to achieve strategy and business objectives.
- **External Stakeholders:** Any parties not directly engaged in the entity's operations but who are affected 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) Governance and Culture; (2) Strategy and Objective-Setting; (3) Strategy and Objective Performance; (4) Review and Revision; and (5) Information, Communication, and Reporting.
- **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.
- **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:** Anything inside of the entity that influences the ability to achieve 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.
- **Operating Structure:** The way the entity organizes and carries out its day-to-day operations.
- **Opportunity:** An action or potential action that creates or alters goals or approaches for creating, preserving, and realizing value.
- **Organization:** The term used to collectively describe 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:** The measurement of 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 managing risk.
- **Reasonable Expectation:** The amount of risk of achieving strategy and business objectives that is appropriate for an entity, recognizing that no one can predict risk with precision.
- **Risk:** The possibility that events will occur and affect the achievement of strategy and business objectives. NOTE: "Risks" (plural) refers to one or more potential events that may affect the achievement of objectives. "Risk" (singular) refers to all potential events collectively that may affect the achievement of 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 Inventory:** All risks that could impact an entity.
- **Risk Profile:** A composite view of the risk assumed at a particular level of the entity, or aspect of the business that positions management to consider the types, severity, and interdependencies of risks, and how they may affect performance relative to the strategy and business objectives.
- **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.
- **Tolerance:** The boundaries of acceptable variation in performance related to achieving business objectives.
- **Uncertainty:** The state of not knowing how or if potential events may manifest.
- **Vision:** The entity's aspirations for its future state or what the organization aims to achieve over time.