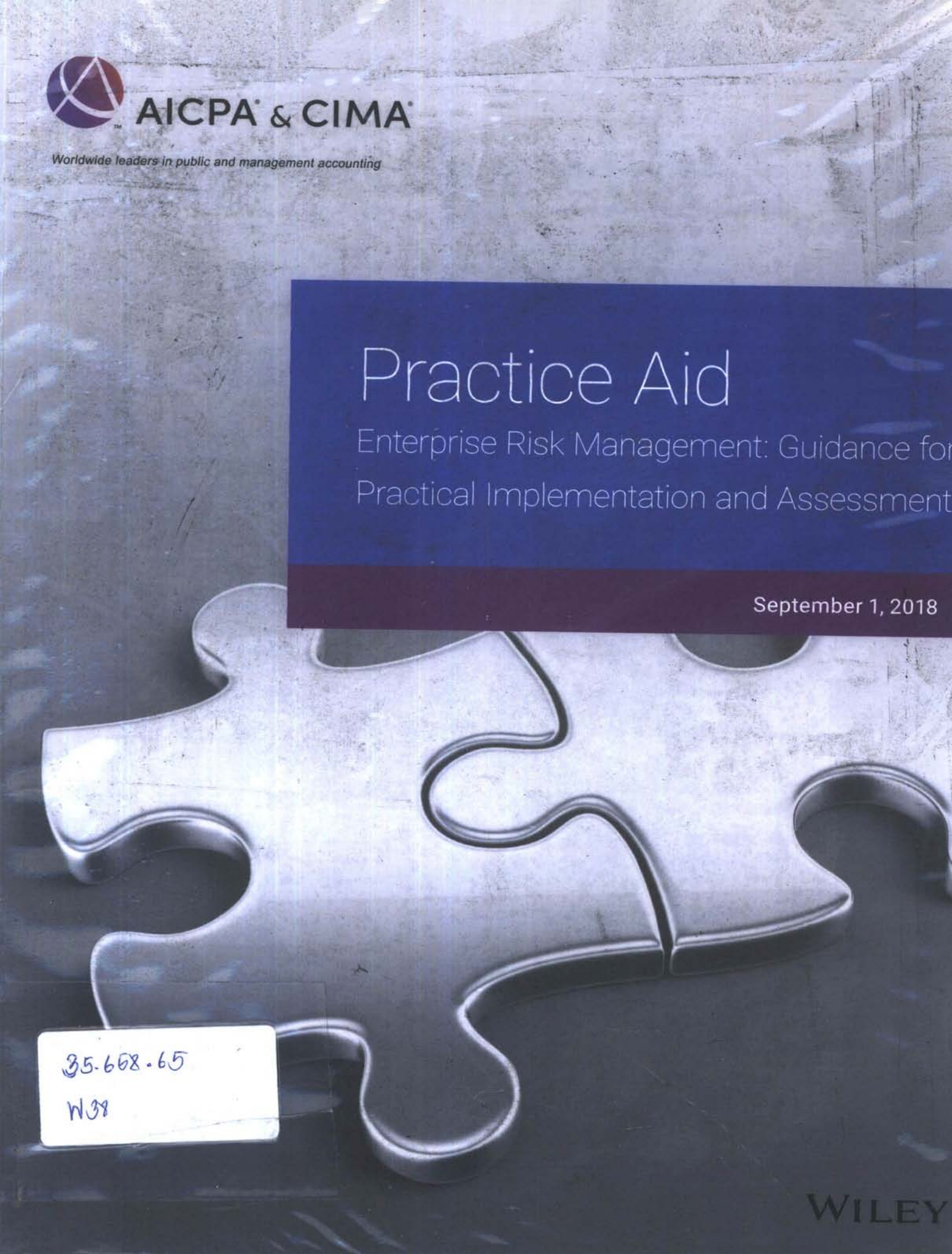

AICPA & CIMA
Worldwide leaders in public and management accounting
Practice Aid
Enterprise Risk Management: Guidance for
Practical Implementation and Assessment
September 1, 2018
35.658.65
W38
WILEY

AICPA & CIMA

Worldwide leaders in public and management accounting

Practice Aid

Enterprise Risk Management: Guidance for Practical Implementation and Assessment

September 1, 2018

23574-349

V10005715_110218

ISBN 978-1-94830-636-2 (print)

ISBN 978-1-94830-637-9 (ePub)

Recognition

Assurance Services Executive Committee (2017–2018)

Robert Dohrer, *Chair*
Bradley Ames
Christine M. Anderson
Nancy Bumgarner
Jim Burton
Mary Grace Davenport
Chris Halterman
Jennifer Haskell
Elaine Howle
Brian Martin
Brad Muniz
Joanna Purtell
Miklos Vasarhelyi

Risk Assurance and Advisory Services Task Force (2013–2014)

Alan Anderson, *Co-Chair*
Suzanne Christensen, *Co-Chair*
Aron Dunn
John Farrell
Bailey Jordan
Leslie Murphy
Tom Patterson
Paul Penler
Sallie Jo Perraglia
Dietmar Serbee
Beth A. Schneider
Leslie Thompson

Additional Contributors

Anita Dennis

Enterprise Risk Management: Guidance for Practical Implementation and Assessment
Revision Contributor (2017–2018)

Suzanne Christensen

AICPA Staff

Charles E. Landes
Vice President
Professional Standards Team

Amy Pawlicki
Vice President
Assurance and Advisory Innovation

Ami Beers
Director
Assurance & Advisory Services — Corporate Reporting

Dorothy McQuilken
Senior Manager
Audit Data Analytics and ERM

TABLE OF CONTENTS

Chapter 1
Overview of the Enterprise Risk Management Publication

I. Introduction

Every organization[1] exists for the purpose of creating value for its stakeholders. To create value, an organization sets objectives, develops strategies, and plans for pursuing them, and performs actions. However, strategies, plans, and actions alone do not guarantee a desired outcome. Events and circumstances could affect the execution of these strategies and plans. Management is faced with the challenge of dealing with the uncertainties surrounding the achievement of its objectives. Enterprise risk management (ERM) is a process that enables management to address these uncertainties in a comprehensive, integrated, and organization-wide manner in order to create value. By implementing and maintaining an effective ERM program, management teams and the governing bodies of those organizations can increase their confidence that the organization can be successful in achieving its objectives. Customers, vendors, regulators, rating agencies, and other stakeholders are increasingly interested in understanding an organization's ERM process and may base decisions regarding their interactions with the organization on the perceived sophistication and effectiveness of the ERM process.

This publication is intended to help those responsible for an ERM program, whether the program is in its early stages or is already well established, to design and operate an effective ERM program.

To begin, it is helpful to understand what an ERM program encompasses and how it is defined. The Committee of Sponsoring Organizations of the Treadway Commission (COSO), in its 2017 *Enterprise Risk Management—Integrating with Strategy and Performance* publication, defines ERM as follows:

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

In comparison, the International Standardization Organization (ISO) 31000, *Risk Management—Guidelines*, defines risk management as "coordinated activities to direct and control an organization with regard to risk" and further explains a risk management process as a "systematic application of policies, procedures and practices to the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risk."

For purpose of this publication, an *ERM Program* is defined as an organization's ERM culture, capabilities, and practices, including its people, structures, governance mechanisms, documents, values and incentives, data, and supporting technologies that allow an organization to operationalize and execute its end-to-end ERM programs. Many organizations are challenged with the initial design and implementation of such an enterprise-wide risk management process and program and with maintaining and improving them over time so that they continue to operate effectively and add value.

Thus, the purpose of this publication is to leverage these two existing conceptual frameworks and provide practical guidance for designing and implementing a new ERM program along with the policies and procedures that define an entire ERM program, or for assessing and improving an existing program. This publication intends to serve as a bridge between the substantial, conceptual guidance that exists today and the practical realities of creating and sustaining a successful ERM program.

[1] **organization**. Any form of for-profit, not-for-profit, or governmental body. An organization may be publicly listed, privately owned, owned through a cooperative structure, or any other legal structure.

II. Who Should Use This Publication

This publication is intended for practitioners who are implementing a new ERM program or improving an existing program. This publication provides a summary of the concepts and components of a successful ERM program and provides a maturity matrix and self-assessment guidance that may be helpful for practitioners who are implementing or improving an ERM program. This publication may also be helpful to third parties who have been asked to provide an evaluation or assessment of an ERM program, such as auditors, compliance specialists, consultants, or other mandated parties. Internal or external auditors in particular may be called upon to independently evaluate the effectiveness of the organization's ERM program and to make meaningful recommendations for improving or enhancing the program.

The ERM concepts, components, and examples presented in this publication are intended to be industry agnostic and applicable to organizations of many sizes and types — including public, private, not-for-profit, and government organizations. An ERM program, however, may vary significantly by industry and organization, and aspects of this publication may be more useful to some organizations than others. Careful consideration should be given to the specific circumstances of each individual organization to ensure that the targeted ERM program is well-suited for the organization.

III. Conceptual Basis for This Publication

The concepts used in this publication are primarily developed based on two of the most well-known risk management frameworks, the COSO *Enterprise Risk Management—Integrating with Strategy and Performance* framework (the COSO ERM framework) and the ISO 31000 *Risk Management—Guidelines* (the ISO 31000 framework). This publication does not create a new framework but leverages the foundational concepts of these existing frameworks. To begin, this publication highlights overarching concepts of ERM, which are foundational to the ERM process and to the rest of this publication. In subsequent sections, the publication discusses in greater detail these concepts and the ERM process by leveraging COSO's framework of components and principles with comparisons to the ISO 31000 framework. A more detailed mapping of COSO ERM framework components and ISO's 31000 framework can be found in appendix A, "COSO and ISO 31000 Framework Mapping."

About the COSO and ISO Risk Management Frameworks

The June 2017 COSO *Enterprise Risk Management—Integrating with Strategy and Performance* publication provides guidance on the broader subject of enterprise risk by defining and explaining key ERM concepts, components, and principles.

The ISO 31000 *Risk Management—Guidelines of 2018* provides principles, framework, and process guidelines on managing risks faced by organizations. The document includes an approach for managing different types of risks and can be applied to any activity at all levels of an organization.

Chapter 2
ERM Benefits, Concepts, and Components

I. Benefits of a Successful ERM Program

The primary focus of an ERM program is to aid an organization in achieving its objectives to ultimately realize value. Thus, the benefits of an effective ERM program are significant.

Strong ERM Gives Companies Higher Market Value

"The Valuation Implications of Enterprise Risk Management Maturity," from the *Journal of Risk and Insurance*, found that organizations exhibiting mature risk management practices realize a value growth potential of up to 25 percent. Using data from the RIMS Risk Maturity Model (RMM), Mark Farrell, Actuarial Science and Risk Management Program Director at Queens University Management School of Belfast (QUMS) and Dr. Ronan Gallagher of the University of Edinburgh Business School, provided evidence that firms that have reached mature levels of ERM qualities exhibit a higher firm value.

Although the previous example is geared toward for-profit organizations, the broader benefits of a successful ERM program accrue to organizations of all types including not-for-profit and governmental. The more specific benefits of implementing and maintaining a successful ERM program include

- increasing the range of opportunities available to an organization to achieve its mission and business objectives.
- reducing surprises not only in individual areas of the organization but across the enterprise. Risks in one part of the organization can create risks to other areas, and ERM helps to proactively identify and manage these risks.
- enhancing overall organization performance by increasing the likelihood of achieving the organization's strategic and operational objectives and reducing performance variability that can create organizational disruption.
- improving capital and resource allocations by providing better information to assess the costs and benefits in these decisions.
- increasing organizational adaptability and resilience by helping the organization identify and respond to external and internal change in a more timely and embedded manner. Risk exists in almost every decision. Thus, in order to be adaptable and resilient, it is essential that risk management is integrated fully into decision-making throughout the organization.

To add value, however, an ERM program must be effective. Thus, it is important to understand the answers to the following two questions:

- What are the attributes or characteristics of a successful ERM program?
- How do I know that an ERM program is effective?

To answer these questions and achieve the overall objectives of this publication, this chapter provides an overview of the ERM concepts and components that compose the ERM framework and are important to a well-functioning ERM program. In addition, subsequent chapters provide practical guidance to create a

reference guide to design and implement, or evaluate and improve, the ERM practices of an organization to ultimately contribute to the success of the organization.

A Successful ERM Program

"Properly designed and implemented, the risk management framework will ensure that the risk management process is a part of all activities throughout the organization, including decision-making, and that changes in external and internal contexts will be adequately captured." (ISO 31000 *Risk Management—Guidelines*, Section 5.5, "Implementation")

It is important to note that no two organizations are alike and, to be successful, an ERM program must be tailored to the specific culture, attributes, and needs of the organization. An ERM program is also not a "check-the-box" or "complete a checklist" activity, as considerable organizational participation and judgment is required. As such, this publication describes the key concepts and components of an effective ERM program along with practical guidance on how to implement or evolve these concepts in a goal of creating an organizationally appropriate ERM program and achieving program success.

II. ERM Concepts

The following section provides an overview of key ERM terms and concepts that are essential to a successful enterprise-wide risk management program.

Definition of ERM

The COSO ERM framework defines ERM as the "culture, capabilities, and practices, integrated in strategy-setting and performance that organizations rely on to manage the risk in creating, preserving, and realizing value." Similar to the ISO 31000 framework, the COSO definition stresses that the goal of ERM is to better enable the organization to manage uncertainty and meet its objectives to ultimately realize value.

Risks and Opportunities

The linkage between these concepts and how they affect an organization's ability to meet its objectives are well established in both frameworks. Although the COSO ERM framework observes that risk is the possibility that events will occur and affect an organization's ability to achieve its established strategy and business objectives, it also notes that an effective ERM program can increase the range of opportunities available to an organization. For example, an organization may determine after assessing its current risks that it is not taking enough risk and by accepting more risk, the organization has more available business opportunities to pursue.

The ISO 31000 framework defines risk similarly as the effect of uncertainty on objectives where an effect is a deviation from the expected, either positive, negative, or both, that can create or result in opportunities or threats. Due to the uncertainty that underpins risk, it is possible for an event to give rise to a new risk or a new opportunity. For example, stronger than expected sales in one area may cause resource constraints and risks to another area of the organization. In contrast, declining sales in one area might free up resources to allow the organization to pursue a new area of opportunity or growth.

Risk in Strategy and Objective-Setting

The COSO ERM framework stresses the importance of an effective ERM program in increasing the likelihood that an organization will realize its business objectives. Although ERM does not create an organization's business objectives, ERM is integral to developing the strategy that drives those business objectives. ERM increases the range of opportunities to be considered in strategy-setting and increases the likelihood that an organization will be successful in both identifying the set of optimal business objectives and realizing the targeted results.

Perhaps most importantly, ERM helps to ensure that both the chosen strategy and the targeted results will be well-aligned with the organization's mission, vision, and core values.

The Importance of Taking an Enterprise or Portfolio View of Risk

A critical element of an effective ERM program is in its application to the entire organization. The COSO ERM framework begins with the concept that the entire ERM program must be applied across the enterprise to ensure its effectiveness.

> "Every organization faces myriad risks that can affect many parts of the organization. Sometimes a risk can originate in one part of the organization but impact a different part." (COSO *Enterprise Risk Management—Integrating with Strategy and Performance*, June 2017).

Although the ISO 31000 framework does not specifically call for a portfolio view of risk, the framework notes that the risk management process "should be an integral part of management and decision-making" and can be "integrated in the structure, operations and processes of the organization." Moreover, applying this ISO 31000 framework consistently and comprehensively helps to ensure that risk is managed effectively, efficiently, and coherently across the organization.

Risk Appetite, Risk Tolerance, and Risk Profile

Risk appetite, risk tolerance, and risk profile are perhaps some of the more challenging ERM concepts to define and apply in practice, particularly as these terms are sometimes used interchangeably. There are benefits, however, to working through these challenges. The COSO ERM framework defines **risk appetite** as the "amount of risk, on a broad level, an organization is willing to accept in the pursuit of value." Risk appetite sets the range of acceptable organizational practices and outcomes in the development of the organization's strategy.

Risk tolerance is the acceptable variation in performance related to the organization's business objectives. Risk tolerance is expressed in measurable units or ranges of units and, ideally, in the same measures used to define the business objectives. Risk appetite, along with the corresponding risk tolerances, also guides decision-making to establish the acceptable variations in performance relative to the achievement of the organization's strategy and business objectives.

A **risk profile** provides a composite view of risk related to the organization's chosen strategy or set of business objectives and is used to evaluate and select alternative strategies. Developing a risk profile is perhaps a more advanced risk practice based on the concept that risk and performance are not constant, and trade-offs exist. By evaluating risk profiles, an organization considers risk appetite in the context of evaluating these trade-offs between risk and performance, ultimately establishing the targeted risk capacity (that is, risk limit) of the organization to determine an optimal strategy and plan.

In comparison, section 6.3.4, "Defining Risk Criteria," of the ISO 31000 framework discusses the organization's approach to assess and eventually pursue, retain, take, or turn away from risk and further urges its reader to define risk criteria to help "evaluate the significance of risk and to support the decision making process." Understanding when and how to define, communicate, and apply risk appetite, risk tolerance, and/or risk profile can be challenging as these processes are iterative, occurring both at the beginning of the ERM process as well as during the ERM process itself.

Regardless of the terminology used, management is responsible for defining, documenting, and communicating the organization's risk appetite by first creating a statement or series of statements that clearly describes the level of risk that an organization is willing to accept in its ongoing activities and in pursuit of its business objectives. There is no standard approach; some organizations seek to define risk appetite more qualitatively, some define it more quantitatively, and others pursue a blended approach. This publication provides further instruction and illustration on how to define and apply risk appetite and risk tolerance in the "III. Future State Operating Model Design" section of chapter 4, *ERM Program Development*.

Risk Inventory

An effective ERM program requires that an organization create an inventory of its risks in categories and terms that allow for common and consistent understanding to support both appropriate capture and assessment. This risk inventory using standardized terminology is often referred to as a risk taxonomy and without a common risk taxonomy, an organization may be challenged to ensure an enterprise-wide view of its risks. Further, the organization may have difficulty assessing its full portfolio of risks against its risk appetite or as part of its overall risk profile. It is important to note, however, that an organization must guard against creating merely a "risk-listing." The true value of an ERM program is having an active, supporting process that considers the impact of these risks upon the organization's ability to meet its business objectives in both the near and longer-term. An organization may look to leverage available industry guidance as a starting point for developing these risk inventories and supporting risk taxonomy.

Emerging Risks

The concept of an emerging risk is well-established in ERM practice and captures the multiple dimensions of uncertainty that give rise to certain types of risk. Emerging risks are by definition highly uncertain and, thus, difficult to fully identify and assess. As such, continual monitoring of the conditions that give rise to these risks is a critical component of an effective ERM program. Time and effort should be dedicated to ensuring that an organization's ERM program fully considers and captures emerging risks as part of its ongoing risk identification process.

Due to the inherent uncertainty of emerging risk, achieving goals can be difficult, particularly in an environment that is subject to a high degree of change. An effective ERM program that is dynamic, iterative, and responsive to change can improve an organization's ability to respond and adapt to change.

Integration and Embeddedness

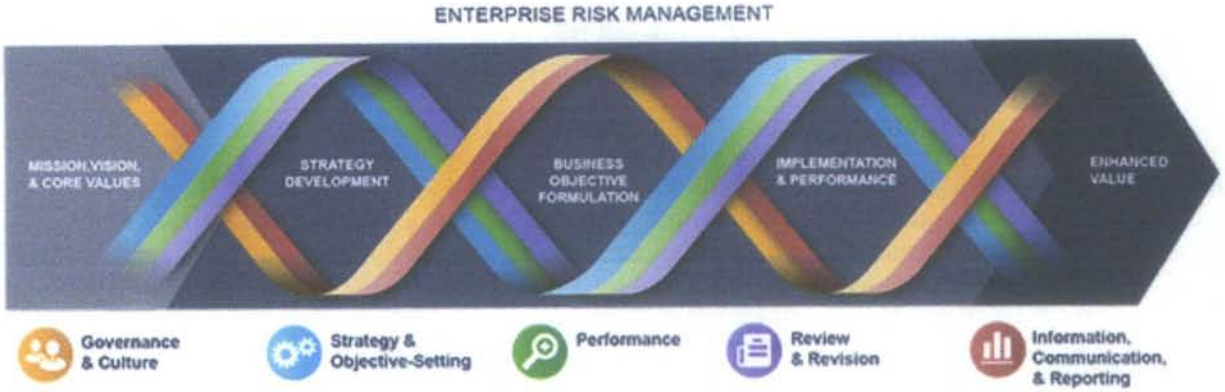
> "An organization can enhance its overall performance by integrating enterprise risk management into day-to-day operations and more closely linking business objectives to risk." (COSO *Enterprise Risk Management—Integrating with Strategy and Performance*, June 2017)

Risk is naturally inherent in an organization's strategy-setting and day-to-day decision making. Thus, to be fully integrated, an ERM program must be embedded in organizational decision-making, rather than operating as a periodic or stand-alone process. Moreover, this integration of ERM must be dynamic and flexible, and the organization must be diligent in evolving its ERM program to be responsive to organizational changes that may affect this integration.

III. Components of an ERM Program

Establishing, maintaining, and continuously maturing an ERM framework is foundational to an effective ERM program. Thus, in order to fully leverage the remainder of this publication, this chapter provides an overview of the COSO ERM framework with reference to the correlated ISO 31000 framework (see appendix A for a detailed, side-by-side mapping of these two frameworks). Similar to the COSO model, the ISO 31000 standard emphasizes the importance of an ERM framework in maintaining an effective ERM program.

To begin, the COSO ERM framework is composed of a set of five interrelated components (see the following diagram), which aligns with the business lifecycle and emphasizes the importance of ERM, from strategy-setting through the realization of value. A properly functioning ERM program is one that is fully embedded in the organization's business activities and decision-making.



The five COSO ERM components are further supported by 20 principles that fully define the COSO ERM framework.

Risk Management Principles

Governance & Culture

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

Strategy & Objective-Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Performance

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

Review & Revision

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues Improvement in Enterprise Risk Management

Information, Communication, & Reporting

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

These components and supporting principles are briefly described in the following pages and are complimented by helpful hints and points to consider when implementing or enhancing an ERM program. As the following section is intended to be an overview, readers are encouraged to reference the full guidance found in the original COSO and ISO documents (COSO *Enterprise Risk Management—Integrating with Strategy and Performance*, June 2017 and the ISO 31000 *Risk Management—Guidelines*, February 2018).

1.0 Governance and Culture

This component includes the following:

- Principle 1: Exercises Board Risk Oversight
- Principle 2: Establishes Operating Structures
- Principle 3: Defines Desired Culture
- Principle 4: Demonstrates Commitment to Core Values
- Principle 5: Attracts, Develops, and Retains Capable Individuals

An effective ERM program begins with well-established governance and operating structures that support a risk-aware and risk-responsive culture throughout the organization.

> "It is widely agreed that failures of culture, which permitted excessive and uncontrolled risk-taking and a loss of focus on end clients, were at the heart of the financial crisis." (*Risk Culture in Financial Organisations, A Research Report*. 2013)

An appropriate governance structure begins with defining the oversight role of the board of directors (or similar organizational oversight group) and ensuring that the board members are sufficiently independent and qualified to provide such oversight. Additionally, board members should be adequately equipped and enabled to challenge the organization's management, whose responsibility it is to maintain a risk-aware organization and ensure execution of an effective ERM program.

The organization's management is fully accountable to the board for establishing an appropriate risk culture and a "tone at the top" that is aligned with the organization's core values and ethical principles. Establishing a risk-aware culture is critical to defining risk management expectations promoting desired behaviors and holding members of the organization accountable for those behaviors. Management is also responsible for communicating these expectations throughout the organization and fostering a culture that promotes open and transparent discussions of risk in both strategy-setting and day-to-day decision-making. Focusing on the value that ERM can deliver, as well as the new opportunities that it can uncover, can assist in addressing any negative connotations that may exist and promote engagement openness and transparency.

Point to Consider: Although culture is understandably difficult to fully articulate and measure, the importance of culture in driving day-to-day behaviors necessitates that management set appropriate expectations and find means for monitoring and measuring conformity with these expectations. This focus is particularly important when the business is affected by heightened organizational change (for example, large initiatives, reorganization, or mergers). Focus should also be placed on activities or functions that create potential conflicts of interest with management's expectations, and safeguards and/or controls should be implemented to prevent and timely detect such conflicts.

Lastly, management is responsible for establishing overall operating structures that provide appropriate competency and sufficient resourcing to achieve its strategy and business objectives. It is also management's responsibility to carry out its risk functions and activities in support of achieving those objectives.

2.0 Strategy and Objective Setting

This component includes the following:

- Principle 6: Analyzes Business Context
- Principle 7: Defines Risk Appetite
- Principle 8: Evaluates Alternative Strategies
- Principle 9: Formulates Business Objectives

Establishing an appropriate strategy to deliver upon an organization's mission and vision begins with understanding the business context in which the organization exists. This context includes broad external factors, such as geo-political, social, economic, competitive, legal, and regulatory considerations. Internal factors include people, processes, systems, and capital priorities or limitations as well as the expectation of the organization's stakeholders.

To identify an appropriate strategy for an organization, management must also understand the organization's overall risk profile (that is, the current aggregate level of risk across the enterprise) and its risk appetite (that is, the amount of risk the organization is willing to accept in pursuit of its strategy). When selecting a strategy, management should evaluate how the strategy affects the risk profile and compare the impacted risk profile to the organization's risk appetite. As a result, the strategy-setting process can be dynamic and iterative to maximize opportunities for delivering value within in an organization's overall risk capacity (that is, the maximum risk an organization is willing to take in the pursuit of its strategy). This process allows the organization to evaluate, assess, and select a strategy that will maximize results.

As previously noted, defining and applying risk appetite is one of the more challenging risk principles as there is no set standard that fits all organizations. Articulating risk appetite requires consideration of both qualitative and quantitative measures, which can be challenging because qualitative characteristics are often difficult to measure and monitor. Further, consideration must be given to tailoring risk appetite to the organization's culture and decision-making environment for it to be most effective for the organization.

Point to Consider: Ensuring that an organization's statement of risk appetite is complete and comprehensive can be challenging. The risk appetite should consider all activities and functions of the organization and correlate to the risks that the organization identifies in its risk identification and assessment process. Standard risk categories and taxonomies, as discussed earlier, can be helpful in identifying whether the risk appetite is complete and to ensure that reported risks can be compared to an organization's risk appetite to establish degree of comfort with the risk ranking, risk priority and targeted risk mitigations as explained in later sections in this chapter.

Point to Consider: Establishing the risk appetite statements themselves can be challenging particularly for risks that require a more qualitative approach (for example, governance risks and culture-related risks). Before finalizing these statements, an organization may find it helpful to identify the key risk indicators (KRIs) relevant to measuring and monitoring risk and to establish risk tolerance ranges (that is, the range of acceptable high or low limits, or both, for the identified KRI). This process can help inform the language used to describe the risk and related risk appetite. Moreover, regular reporting of KRIs with the associated risk tolerance can help the organization monitor whether it is operating within its targeted risk profile and whether it can ultimately achieve its strategic and business objectives.

To implement a strategy, an organization must define the supporting business objectives and their related performance measures to ensure that that the objectives are well-aligned with the selected strategy. The COSO ERM framework notes that there are several strategy-related risks that an organization should consider when developing its ERM process. Strategy-related risks can include

- the risk that the targeted strategy does not fully align with the organization's mission, vision, and core values, and
- the risk of unintended outcomes from the selected strategy (that is, risks of the chosen strategy), or
- the risk that the organization will not fully achieve its chosen strategy (that is, risks to the strategy).

Lastly, organizational bias exists in every strategy-setting process, so it is critical for an organization to identify ways to mitigate such bias. To do so, an organization can start by evaluating and challenging the assumptions underlying the selected strategy. Such assumptions might include assumptions about the business context, industry changes affecting the organization or client demands, assumptions regarding organizational capabilities or readiness, or resource availability.

3.0 Performance

This component includes the following:

- Principle 10: Identifies Risk
- Principle 11: Assesses Severity of Risk
- Principle 12: Prioritizes Risks
- Principle 13: Implements Risk Responses
- Principle 14: Develops Portfolio View

> "Managing risk is iterative and assists organizations in setting strategy, achieving objectives and making informed decisions." (ISO 31000 *Risk Management—Guidelines*, February 2018)

The performance component of the COSO ERM framework captures the process for identifying, assessing, and mitigating risks that could affect the organization's ability to achieve its strategy and related business

objectives. This component includes the ERM practices of identifying risks, assessing the severity of the risks across several measures, prioritizing the risks based on severity to determine the most effective risk responses, and then implementing those risk responses.

The size, complexity, and decentralized vs centralized nature of the organization will dictate the level of design or enhancement that will be required for these ERM performance-based principles. Regardless of the particular approach taken by the organization, there are critical points to consider that are highlighted in the remainder of this section.

The first principle, Identifies Risk, suggests that an organization begins by creating a standard inventory of risks to the organization described and documented using a risk taxonomy of standard categories and definitions. Such a risk inventory, which is sometimes referred to as a risk register, facilitates a common understanding of risks, ensures that everyone is discussing and debating the same risks, and allows for improved categorization and roll-up of risks across the enterprise. This common risk language also supports risk dialogue and awareness across the organization.

Benefits of a Standard Risk Taxonomy

A well-developed risk taxonomy defines categories of risks or risk attributes to

- provide a common language for identifying and assessing risks;
- identify risk patterns or similarities across the organization for optimal analysis and monitoring;
- allow aggregation of risk across an organization, cutting across business lines or boundaries; and
- provide clarity in communication and reasoning, and better enable the management of risks across the organization.

Point to Consider: It is helpful to develop a list of well-defined, discrete risks that are not too broad or too narrowly-focused. If risks are too broad, the organization will struggle through the assessment process as well as how to effectively mitigate or identify who is accountable for the mitigation activity. If risks are too narrow, the full impact of the risk may not be captured or may be underestimated.

Point to Consider: It is also helpful to define and describe the risk in terms of the impact of the risk to the organization. This can help the organization better understand how to mitigate the risk and determine who is accountable for the mitigation efforts. Moreover, certain external risks, such as the risk of a market downturn, cannot be controlled directly by the organization. The identified risk of the market downturn, however, can be described in terms of the resulting or follow-on risk to the organization. In this example, a market downturn might cause a loss of client demand for the organization's products or services and the resulting risk to the organization would be described in terms of the lost client revenue due to a market downturn.

Point to Consider: During the risk identification process, it is critical to not only include known risks, which are typically based on historical data and actual events, but to also consider the possibility of unknown future risks. It is also important to consider risks with a longer time horizon. For example, failure to identify new products or services based on changing customer demands may not be a significant issue in the short-term but may create a risk of customer irrelevance over the long-term.

Point to Consider: It is also important to ensure that business change is considered in the risk identification process. Care should be taken to timely monitor external and internal changes that can give rise to significant risk and prevent the achievement of business objectives. Often, significant change can develop incrementally over time and may be more difficult to identify in real-time.

The next principle defines the process for assessing the severity of risk. This process involves capturing and considering all the dimensions of the risk in order to prioritize and select an appropriate risk response and mitigation plan. Such dimensions include (but are not limited to) severity measures such as

- likelihood or probability that the risk will occur over some specified time frame,
- residual impact of the risk after considerations of the risk controls over the time frame described,
- target residual impact of the risk after considering risk appetite,

- risk trend or velocity (for example, increasing, stable, or decreasing), and
- risk persistence (that is, how long the risk will persist post initial occurrence).

There are multiple approaches that can be employed to conduct a sound risk assessment process. However, considerable expertise and judgment may be required as certain combinations of the measures can result in a range of potential outcomes. Ultimately, this process should capture results that lead to the highest potential risk and the associated risk response. In some cases, it is helpful to capture more than one outcome because the risk response might vary by outcome.

Lastly, consideration should be given to when the assessment process should be repeated across the entire inventory of risks or for a subset of risks. Factors that may influence when the assessment process is repeated include a change in the external business context, a change in the strategy or objectives of the organization, or other external or internal changes. The process should be revisited on a recurring basis (for example, annually or quarterly) to ensure that appropriate consideration is given to changes in the internal or external environment that could affect the organization.

Benefits Gained from a Sound Risk Assessment Process

- Ensuring risk awareness and appropriate dialogue across the company
- Understanding how divisional risks affect overall company risks
- Identifying synergistic risks that increase the probability or impact of risks
- Preventing risk "silos" and increasing transparency of divisional risks
- More timely identification of emerging or unexpected risks
- Improving the likelihood of achieving strategic objectives and prioritizing plans and actions
- Supporting a process for continuous improvement

After the risk assessment process is complete, risks are then prioritized in order to determine appropriate risk responses. Criteria must first be established as a basis for prioritizing risks. Common criteria used for prioritization include risk severity and risk trend (that is, increasing, decreasing, or stable). Organizations, however, may also consider other factors relevant to their business such as impact to strategy or objectives. The risk prioritization process also provides a basis for ongoing reporting and monitoring of risks to ensure that the organization is focused on its most important or critical risks.

After the risk assessment and prioritization process is complete, the organization identifies an appropriate risk response, such as those noted in the following box. Choosing an appropriate risk response includes careful consideration of the cost and benefits of each response, which may vary based on the timeframe required for the response. In some cases, the organization may choose to employ more than one response (for example, one for the short-term and another for the long-term, or some combination more permanently), which may require a more iterative process.

Types of Risk Responses

accept. A decision to take no action to address or further mitigate a risk. Risks that are accepted should generally have low impact on the organization.

avoid. A decision to remove the risk entirely by stopping or eliminating the activity that gives rise to the risk.

pursue. Action is taken that accepts increased risk to achieve improved performance.

reduce. A decision to address a risk by developing and implementing additional or better controls to counter the underlying threat or to minimize the resulting impact, or both. Risks that are further mitigated are those that typically have a medium to high impact on an organization.

share. A decision to mitigate the impact of the risk to the organization by sharing the risk with an external party (for example, an insurance company).

Point to Consider: Establishing an appropriate risk response should include plans for managing through potential crisis-level risks, particularly those risks that cannot be fully mitigated to within an organization's risk appetite (for example, cyber risks). Pre-planning for a crisis scenario ensures that the organization can quickly and effectively respond with a goal of getting back to business as usual as soon as possible. Important to these plans is full consideration of timely communication with internal and external stakeholders, in particular the board, as many crisis situations have been made far worse due to poor and/or delayed communication.

After the risk assessment, prioritization, and response process is complete, risks can be presented in a risk dashboard, heat map, or similar type of report to visually represent the relative ranking of risks. Other measures of risk could be included, such as likelihood, impact, and trend or persistence (that is, the length of time a risk may be present once triggered). These types of visual presentations can help to focus the organization on risks that are not well aligned with its overall risk appetite and further support discussion of how best to appropriately manage, mitigate, and monitor risks.

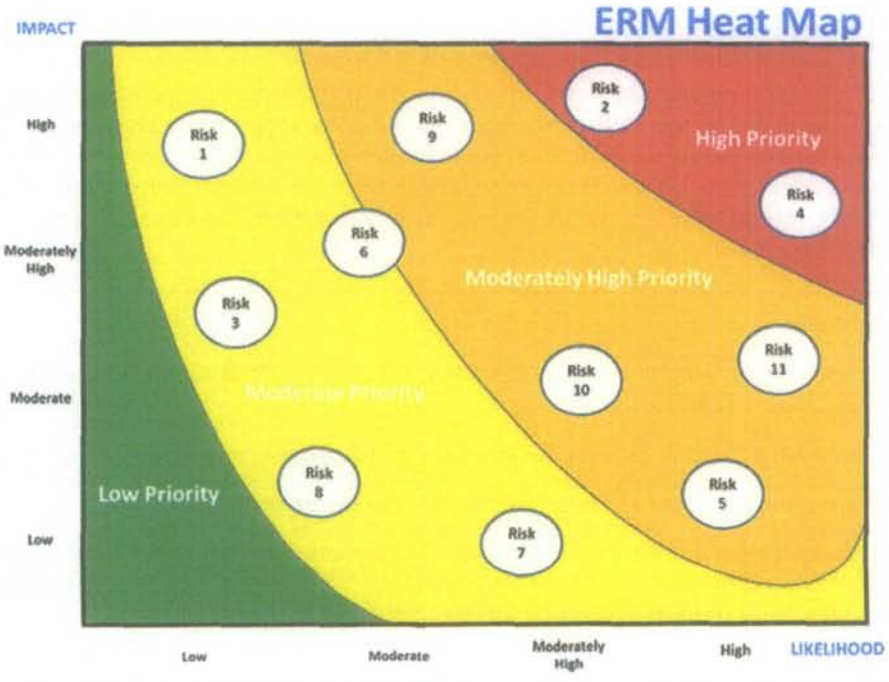
ERM Heat Map Definitions and Scales

Establishing the definitions and scales for reporting and prioritizing the organization's most significant risks requires both judgment and discussion. The goal of the heat map is to support an understanding of the results of the risk assessment process and facilitate an active dialogue on how those results compare to the organization's overall risk appetite to determine what further actions might be required.

The following heat map provides a simplistic example of a heat map that captures risk impact and probability where

- **impact** is based on quantitative measures (for example, financial losses and lost opportunities) of a risk occurrence, although such values can be difficult to assign particularly where the more severe impacts are to the organization's reputation.
- **likelihood** is the chance that this risk will occur during the assessed time period. Sometimes the term *probability* is used.

The following heat map assumes that the organization's risks are presented post-completion of a risk prioritization review that excludes any low priority risks from the heat map.



The performance component of the COSO ERM framework emphasizes the importance of taking an enterprise or portfolio view of risks. Taking an enterprise or portfolio view of risk requires that an organization develop a "rolled-up" view of risk across the enterprise. In doing so, considerable judgment is required as some risks actually increase in severity as they are consolidated across the organization. Conversely, some risks may naturally offset or even mitigate each other in the portfolio. The ultimate objective is to look for undue concentrations of risk or identify areas of natural diversification that aid in mitigating risk and to consider these concentrations as part of the full ERM program.

The portfolio view of risks should be compared to the overall risk appetite of the organization to ensure that the organization's current risk profile does not exceed its overall risk appetite or that there is a not an opportunity to take additional risks to maximize opportunity. Ideally, the rolled-up view of risk should also be compared to the organization's business objectives and strategy to ensure an appropriate focus on achieving strategy and to aid in identifying multiple risks to a single business objective. This process ultimately supports ongoing monitoring of performance and decision-making.

Point to Consider: The true value of the entire risk management process is derived from robust and open dialogue alongside a true challenge process to guard against undue bias, group think, and blind spots. Ensuring that the process leverages appropriate subject-matter experts at every stage improves the quality of the ERM results in both the nearer and longer term.

4.0 Review and Revision

This component includes the following:

- Principle 15: Assesses Substantial Change
- Principle 16: Reviews Risk and Performance
- Principle 17: Pursues Improvement in Enterprise Risk Management

As mentioned in the last principle, considering external and internal changes that affect an organization's ability to achieve its strategy is critical to an organization's success. The principles found in this component stress the importance of considering change in all aspects of an ERM end-to-end process and stress that such consideration should be integrated into the ongoing business practices in order to be fully effective. This includes considering changes that affect not only the strategy and the business objectives but also the underlying assumptions in both.

To adequately consider the impact of change and respond accordingly, the organization should look to review its performance against the performance targets established for both the strategy and business objectives. Such a review will identify areas that require further review, corrective actions, change in approach, or areas of new opportunity.

Finally, a review of organizational performance should include a review of the ERM capabilities and practices themselves to ensure that the organization is continuing to evolve and mature its ERM program to achieve its intended value to the organization.

5.0 Information, Communication, and Reporting

This component includes the following:

- Principle 18: Leverages Information and Technology
- Principle 19: Communicates Risk Information
- Principle 20: Reports on Risk, Culture, and Performance

This last principle focuses on the importance of ongoing communication and reporting to an effective ERM program. Such reporting should consider all stakeholders and encompass all areas, activities, and outcomes of an ERM program.

ERM reporting should include

- a portfolio view of the organization's risks with appropriate prioritization and ranking (for example by using the earlier heat-map for presentation).
- key risk and performance indicators to assess the degree to which the organization is operating within its overall risk appetite and profile and to measure and report on risks to the organization's strategy and business objectives. This reporting should also consider risks to the underlying assumptions to the strategy and objectives and typically includes both quantitative (for example, errors or losses) and qualitative measures (for example, measure of employee values).
- risk response actions and plans and their status or achievement.
- the process for capturing new or emerging risks as well as the results of this process.
- risk management program evaluations, recent enhancements, and improvement plans.
- risk awareness and culture reporting (note that this reporting is generally qualitative in nature.

ERM reporting should be timely and relevant and is ideally supported by leveraging data that already exists in the organization. Obtaining information from sources already included in regular management reporting has the added benefit of directly tying into existing management reviews and oversight processes rather than requiring incremental monitoring. Although historical information is helpful, forward-looking information or early-warning indicators are most beneficial.

Finally, it is important to implement feedback and escalation paths as part of the ERM reporting process to allow for the communication of issues, as appropriate, to ERM sponsors, business leaders, and oversight groups.

Chapter 3
ERM Roles and Responsibilities

Although specific roles and responsibilities for designing, implementing, maintaining, and evaluating an ERM program are mentioned throughout this publication, this chapter summarizes the roles and responsibilities critical to an effective ERM program by leveraging specific guidance found in both the COSO ERM and the ISO 31000 frameworks. This guidance includes roles and responsibilities specific to governance, oversight, and ongoing accountability essential to maintaining an effective ERM program. It is important to note that the structure and assignment of specific ERM responsibilities may differ depending on an organization's size, complexity, and resource availability.

> "Culture is developed and shaped by the people at all levels of an organization by what they say and do." (COSO *Enterprise Risk Management—Integrating with Strategy and Performance*, 2017)

I. Organization Roles

Board or Equivalent Roles

The organization's board of directors or similar governance group is responsible for providing appropriate oversight of an organization's ERM program. This oversight responsibility should be documented in the governance or charter documents, which should reference the following:

- The board or governance group composition supports diversity of thought which facilitates appropriate challenges in strategy setting and other discussions with management.
- The board regularly receives communications from management on the portfolio view of significant risks affecting the organization's performance, a comparison of these risks to the organization's risk appetite, and how the organization is actively monitoring and managing these risks with particular emphasis on those that are not fully within the organization's risk tolerance.
- In addition, the board regularly reviews the organization's risk management program and outcomes and how the organization achieves its risk management objectives.
- This oversight process is documented in meeting agendas, minutes, and other materials.

Some boards establish an ERM subcommittee and others combine risk oversight with audit or finance subcommittees; however, due to the linkage between strategy setting and the achievement of business objectives, full oversight responsibility should remain with the entire board (or equivalent governing body). As such, the board's oversight should include the following:

- A full board review of the ERM program that takes place at least annually to ensure that the board or governing body is sufficiently knowledgeable about the organization's ERM program and outcomes, including its processes in place to monitor risk awareness and risk culture
- Awareness of and concurrence with the organization's risk appetite statement and risk tolerances, as evidenced by reviews and approvals
- Regular updates on the organization's most significant risks with a particular emphasis on those risks that may affect the organization's strategy or achievement of its business objectives

- Regular review of the organization's portfolio view of risks relative to its risk appetite and tolerances along with a review of the processes in place to monitor and manage those risks

Organization Management

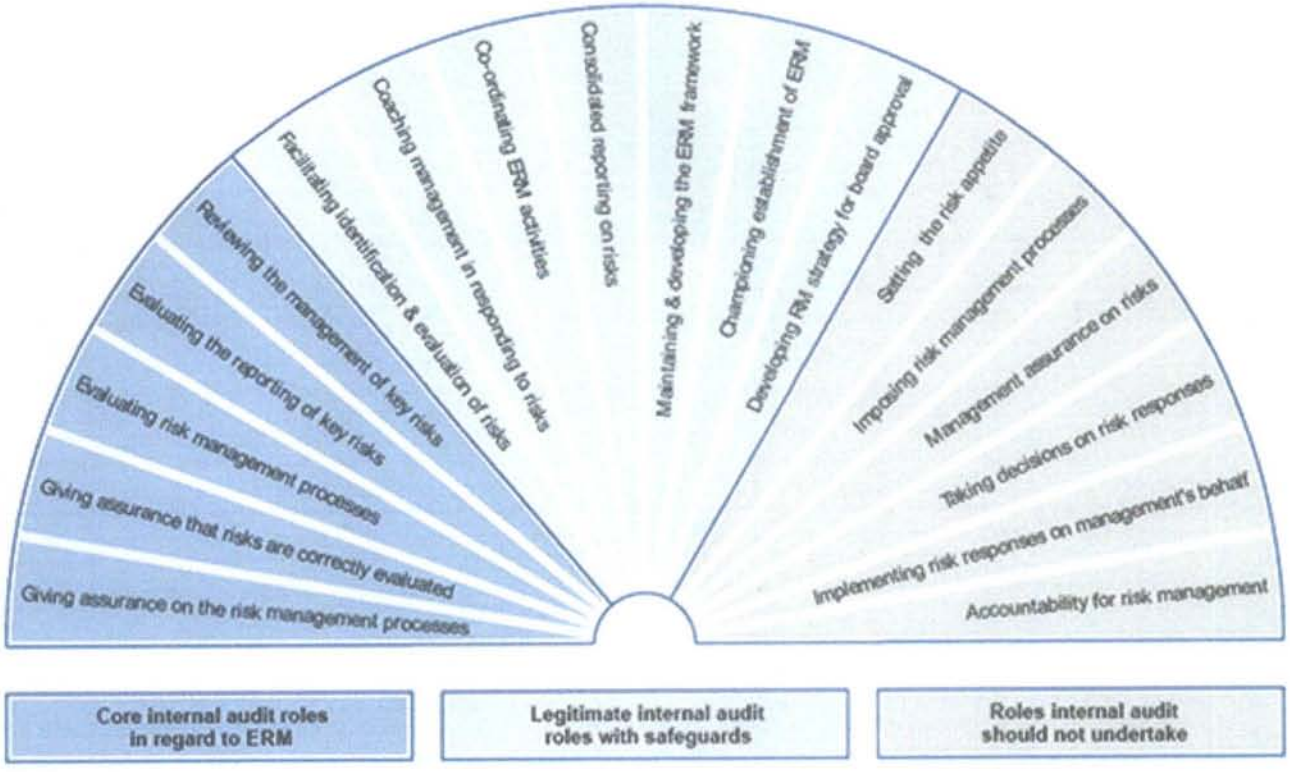
The organization's management, under the leadership and guidance of its chief executive, is responsible for all ERM activities and for ensuring that ERM responsibilities are well communicated and understood (that is, through training) throughout the organization. As such, management should take action in support of the following:

- There is an appropriate risk culture and awareness including the "tone at the top" and "tone in the middle" that discourages improper activities and establishes opportunities to report issues outside of normal reporting lines.
- ERM is embedded in day-to-day decision-making and is understood to be everyone's responsibility and as such is an explicit and implicit part of everyone's job description and performance standards.
- Senior management and risk owners have responsibility for managing risks related to the organization's objectives and activities.
- ERM responsibilities are cascaded throughout the organization, with each manager accountable to the next level of management.
- Compensation plans discourage undue, inordinate, or inappropriate risk-taking.
- There exists appropriate ERM governance and allocation of resources (for example, dedicated committee or function, adequate funding for prioritized mitigation efforts) for the ERM program to be effective.
- Risk management activities are structured to ensure enterprise-wide risk management and avoid risk "silos."
- Quality review programs, which are often supported by internal audit or compliance functions, provide reasonable assurance that the ERM program is effective and operating as designed.

An ERM committee or function within the company, with a designated lead, manages and monitors the ERM program and gathers evidence of a well-functioning ERM program, as indicated by the committee agendas, minutes, documented policies and procedures, action or approval logs, and ongoing reporting. Careful consideration should be given to this committee's constituency or structure to ensure enterprise-wide representation, expertise, and participation. The composition might vary depending upon the size, complexity, and nature of the business.

Internal Auditors

Internal auditors can play an important role by conducting assessments of the ERM program and providing assurance on its design and function. Internal auditors can also assess the effectiveness and efficiency of risk responses and related control activities. The following diagram, extracted from The Institute of Internal Auditors (IIA) Position Paper, "The Role of Internal Auditing in Enterprise-wide Risk," illustrates internal audit's potential role in the ERM process and describes tasks that internal audit personnel may perform to ensure that they do not compromise independence or objectivity.



II. The Role of External Parties in the ERM Process

Where appropriate, an organization's management or its governing body may engage parties not responsible for the day-to-day management or oversight of the ERM program (for example, external auditors, advisory firms, and rating agencies) to provide reviews of the effectiveness of the ERM program. Such reviews by external parties should be supported by letters of agreement or understanding and should include reporting expectations.

ERM Program Success Factors

- Executive sponsorship and appropriate culture
- Linkage to strategic initiatives and objectives
- Enterprise-wide perspective, expertise, and involvement
- Detailed, continuous communication
- Clear documentation of the program
- Realistic cost/benefit considerations
- Adequate training and resource allocation
- Commitment to continuously maturing the program

Chapter 4
ERM Program Development

This chapter provides guidance on how to implement a new, formal ERM program and how to enhance an existing one. This chapter builds upon the concepts and components of an effective ERM process described in chapter 2, "ERM Benefits, Concepts, and Components," as well as guidance found in the ISO 31000 Risk Management Guidelines, section 5.5, "Implementation." It also provides guidance on the policies and procedures required to expand an ERM process into a full ERM program and ensure completeness. Although there are many approaches and ways to develop or enhance an organization's ERM program, this chapter provides guidance organized into five phases.

ERM Program Benefits

"Managing risk is imperative for successful leadership in today's business world. Leaders must develop processes like enterprise risk management (ERM) to improve their ability to manage risks effectively. ERM cuts across an organization's silos to identify and manage a spectrum of risks."

Paul L. Walker and William G. Shenkir, *"Implementing Enterprise Risk Management,"* (2008)

Phases in ERM Program Development

I. Mobilize

Mobilize Phase Objective: Engage and formalize senior sponsorship, establish governance mechanisms, define project roles and responsibilities, allocate resources, build out a detailed timeline, and formally launch the project.

This phase provides the opportunity to articulate and confirm the program objectives and benefits, and to design and implement the project infrastructure and governance mechanisms.

At the onset, it is important to recognize and articulate the value of an ERM program for management and other stakeholders. By doing so, the organization can work to ensure that appropriate support and commitment is given by all levels of the organization.

As described in chapter 2, potential benefits of an ERM program include providing a reasonable expectation that the overall strategy and business objectives of the organization will be achieved. In addition, a well-run ERM program will aid in the following:

- Streamlining monitoring, compliance, and control efforts to improve efficiency and effectiveness
- Meeting regulatory, investor, client, and other stakeholder expectations
- Establishing and standardizing an enterprise-wide understanding of ERM to ensure adequate and timely consideration of risk in strategy-setting and operational management activities

It is important to note that identifying, articulating, and realizing the benefits of ERM is an iterative process. Additional benefits of the ERM program may be identified as it is developed or matured.

With that in mind, the following are suggested activities in the "Mobilize" phase.

Establishing Appropriate Sponsorship and Resourcing

The project management team needs to make sure that it has proper sponsorship to make its ERM initiatives successful. There should be adequate and sustainable sponsorship to support the project for the continued success of the ERM program and to ensure sufficient resources, support, and organizational commitment to change.

ERM Sponsorship

From the onset of an ERM program, executive-level sponsorship and strong leadership are crucial, no matter the size of the organization. ERM sponsors and leaders should have the requisite and recognized authority to ensure

- full oversight, transparency, and accountability across all activities of the organization, and
- appropriate participation and resources to make the program successful.

Because an effective ERM program needs to function across the organization, ERM sponsors likely need to be the most senior members of management (C-suite or equivalent). Although sponsors are critically important at the beginning of the program, ongoing commitment and active participation from sponsors is equally important to ensure continued focus and responsiveness to ongoing change.

Commitment of Resources

After establishing appropriate sponsorship, consideration should be given to how to resource the program from initial implementation through ongoing program management and support. With respect to the ongoing resources, the project team should consider the following questions:

- Will there be a chief risk owner, officer, or other equivalent ERM lead, and how and when will this role be introduced into the program?
- Will there be dedicated ERM support roles and, if so, what are those roles and what skills are required in those roles?
- Will a permanent ERM committee be formed and, if so, what organization-wide, cross-functional representation is required? Consideration should be given to ensure that there is full organization coverage, representation from specific risk areas (for example, information technology, finance, and legal) as well as from areas where there are current risk-related roles (for example, compliance and internal audit).
- Who will be involved in the ongoing risk assessment, monitoring, and reporting processes, and how will these individuals be engaged in the ERM program?

Establishing Roles and Responsibilities

In most cases, the program will be developed in phases as ERM roles and related responsibilities evolve and mature over time. The size, complexity, and scale of the organization will also affect the resources required to ensure the ERM program's success. Management will need to ensure that the ERM program fits well within the context of the organization's existing governance and oversight processes and is embedded in its day-to-day operations by including the following:

- Strategy and objective-setting forums
- Day-to-day management committees and meetings
- Permanent oversight committees
- Ad-hoc project committees

Program Governance

Key elements that should be defined for an ERM program include the ERM charter, objectives, governance structure, communication approach, reporting and issue escalation mechanisms, key roles, and responsibilities. Typically, enterprise-wide programs will have a sponsor, steering committee, and dedicated resources to support the ongoing program activities. Initial implementation or key enhancement phases of an ERM program may also require a project manager, and other project resources.

Planning and Launch for an Initial Program Development Phase

This phase begins by conducting a project planning and launch meeting with sponsors, stakeholders, and other interested parties to confirm expectations, high level timing, and other planning-related impacts and considerations. This initial "kick-off" meeting can be helpful to confirm commitments and set expectations from the very beginning of the project to ensure success.

Suggested outputs include the following:

- Project charter, scope, and approach
- Project organizational or resource chart identifying project participants by role
- High-level plan and timeline
- Project communication and change management plan
- Ongoing status reporting and meeting schedule
- Project issue tracking, reporting, and escalation process

Timeline

The timeline for completing the mobilize phase is typically only a few weeks or less, even for more complex organizations.

Initial Questions to Consider During the Mobilize and Plan Phase

- How should the program's value be defined and communicated in the context of the organization?
- How can appropriate sponsorship be ensured?
- Who are the critical stakeholders, participants, and other interested parties to be considered in the initial program development and in the ongoing communication plan?
- What resources are needed for the project to be successful in both the short- and long-term?

- What is the timing and urgency for initial rollout?
- Are there any existing risk management processes, procedures, or tools that should be considered?
- How should progress be reported?
- What dependencies or risks to implementation exist and how will the program address them?

II. Current State Analysis

Current State Analysis Phase Objective: Develop a baseline understanding of the current state of ERM activities and document the current state to help with future project phases.

Understanding the current state and effectiveness of an organization's ERM program will allow it to assess, leverage, and improve upon existing processes. Information gathering is vital during this phase and a key suggested output is an inventory of the organization's existing ERM activities, along with an initial assessment of their current effectiveness. All ERM activities, even those in the process of being implemented, should be included in the current state inventory. Moreover, although the scale and scope of these existing activities may vary widely from one organization to another, organizations typically have some ERM processes in place to identify risks and take steps to better understand and address those risks.

Current State Considerations

The current state phase should consider all the components and principles of an effective ERM program to ensure information gathered covers the entire end-to-end ERM process. The project team should establish protocols for logging the information received and determining the criteria for the review process so there is consistency, especially if there are multiple reviewers.

This current state analysis should be focused on identifying the effectiveness of the components of the existing program and identifying opportunities for more formalization and improvement. For example, the existing ERM program may not have adequate governance or may lack monitoring procedures to ensure the process is effective. Identifying gaps and shortcomings of the current state program provides opportunities for future improvement as well as a baseline against which to measure future success.

Appendix B, "Example ERM Program Maturity Self-Assessment," includes an example of a maturity matrix that can be used to evaluate the current state of the ERM program. This matrix provides *criteria* or *attributes* for evaluating the maturity of the ERM program across the COSO ERM components (as described in chapter 2). The criteria are organized along a maturity scale ranging from level 1, which describes the attributes expected in a program that is in its initial stage of development, to level 4, which describes a more mature program. The results of this evaluation can be used to provide an overall rating of the program, although judgment must be applied as a typical ERM program will not be uniform in its maturity across all of the components.

Consideration should be given to obtaining input and perspectives from management and key decision makers to provide relevant insight into the organization's risk culture and perceived value of the current activities and process as well as opportunities for improvements. Obtaining stakeholder input can also be helpful in identifying emerging risks and risk trends not currently captured as well as promoting awareness of the benefits of ERM and the reasons for formalizing or enhancing the ERM program.

Creating an Initial Inventory of Activities and Outcomes and Gather Documentation

The amount and type of information gathered for the current state analysis can vary greatly by organization. It is therefore helpful to start with a basic organization "map" (for example, function, department, and employees by role) and information request list. Information frequently gathered and reviewed to identify the current state might include the following:

- Organization charts (for example, board structure, committees, and so on), charters, mission statements, and functional overviews
- Business strategy, planning, and risk appetite-setting processes
- Risk and control assessments and measurement approaches
- Sample risk management reports
- Risk management framework, infrastructure, process, or policies
- Initial assessment of the value or benefits derived from the existing ERM activities

Additional sources of information may include the following:

- **Surveys/Self-Assessments** — The organization may choose to send a prepared list of questions or a self-assessment to select representatives in the organization, key risk personnel, internal audit, organization leaders, or others to capture current risk management practices. The advantages of using surveys and self-assessments include a consistent set of questions and information requests that can be disseminated throughout the organization and results which can be easily aggregated. However, note that obtaining timely responses can be challenging when using surveys and self-assessments. Further, with no face-to-face interaction it may be difficult to interpret results or determine the validity of the information provided, thus warranting the use of additional methods.
- **Interviews** — Another method of information gathering is interviewing stakeholders and resources identified during the initial planning meeting. For these interviews, there may be a prepared set of questions used to guide the interview, and it may be helpful to send these questions in advance of the interview. If so, the proposed list of interview questions may be discussed as part of the initial kick-off meeting.

Questions to help you get started

- What do you consider to be the primary value of our ERM program?
- Is the current ERM program effective? Why or why not?
- How can the program be more effective?
- What does it mean to have a risk-aware culture?
- How do you define a risk-aware culture?
- Do we have a risk-aware culture? At all levels?
- Do we appropriately and timely identify emerging risks?
- What can we do to create more challenge in our risk management activities and discussions?

- **Workshops** — Conducting a workshop or several workshops of representatives from the organization, such as key risk personnel, internal audit, or business leaders, may be an expedient method for gathering or validating information. Workshops may be structured by function, ERM process, or other factor, but they should maintain flexibility to adapt to information received during the workshop. Careful consideration should be given to the diversity of representation from the organization

(that is, seniority, level of experience, and scope of roles and responsibilities) to ensure the workshop is effective.

Suggested outputs include the following:

- Inventory of existing ERM activities
- Initial assessment of the effectiveness of current ERM activities
- Current state and initial findings of the validation workshop

Timeline

The timeline for completing the current state assessment is dependent upon the size and complexity of the organization, but a good baseline assumption is several weeks. It is important to maintain project momentum, resources, and support during this phase.

III. Future State Operating Model Design

Future State Operating Model Design Phase Objective: The primary goal of this phase is to design a future state operating model or update an existing operating model for the organization's end-to-end ERM program.

The future state ERM operating model design can be informed by such resources as

- the current state analysis which provides baseline information as well as future state objectives,
- analysis of peer organizations' leading practices or industry guidance,
- the ISO 31000 framework section 5.1, which describes the necessary components of the framework for managing risk and how they relate, and
- regulatory requirements.

The following are suggested activities for this phase.

Peer and Industry Analysis

Typically, comparisons to organizations both within the same industry and outside the industry can be insightful. Organizations within the same industry often have similar organization models and may face similar risks. Comparisons across industries can yield useful data points when the project team is looking for baseline practices and practical guidance from organizations that are more mature in terms of risk management. Additional considerations include the following:

- Baseline practices that consider ongoing scope, scale, and complexity
- Leading or accepted industry standards for effectiveness, efficiency, and benefit realization
- Lessons learned in the industry as a result of industry developments, events, or risk management failures
- Industry regulatory requirements and expectations

The project team, after determining the criteria for the comparison, should determine how the comparison should be documented and subsequently summarized and reported to project sponsors and other interested parties.

Developing a Target ERM Operating Model and Framework

A thorough, formally documented ERM operating model and framework can provide a solid foundation for effective ERM governance and program development. The ERM operating model and framework should articulate the goals, objectives, and value proposition of the program. They should also define the ERM organization and governance structure, risk philosophy and culture, key risk management processes, reporting, and infrastructure in scope for the overall program as follows:

- **ERM organization and governance**
  - — Role of the board or similar governance body in the design, review, and approval of the initial program as well as oversight of the ongoing risk management program
  - — Structure, authority, composition, and mandate of committees that have formal risk management responsibilities
  - — Dedicated ERM resources, roles, and responsibilities
- **Risk philosophy, culture, and appetite** — Risk philosophy and statements defining culture, including the "tone at the top," risk management values, degree of risk taking or avoidance, and risk appetite that guides the execution of roles and responsibilities, day-to-day decision-making, and how the philosophy, appetite, and culture are cascaded throughout the organization.
- **Risk management processes** — Risk appetite and tolerance setting, risk identification, risk measurement, risk mitigation, monitoring, control and validation, and performance measurement and evaluation.
- **Risk analytics, reporting, and infrastructure** — All required ERM reporting including the portfolio of prioritized risks, key risk and performance indicators, risk responses, actions and plans, comparisons to risk appetite and tolerances, and ongoing ERM program reporting.

To ensure comprehensiveness, the initial target ERM model and documentation should also consider how the entire end-to-end organization (for example, all business units, products and services, legal organizations, regions or geographies, and employees) will be considered and included in the scope of the program.

Equally important to comprehensiveness is the need to ensure that the program is appropriately tailored to the organization, as no one size or structure fits all. An effective ERM program needs to be fully embedded in the culture and the activities of the organization. Thus, it is important to consider how the overall organization is managed and how decisions are made (for example, extent of central versus decentralized or matrixed management, hierarchy of key decision makers, existing protocols, or decision-making processes).

The target operating model should be reviewed iteratively with the core ERM project team and sponsors to obtain feedback and ensure support and buy-in.

Developing the ERM Risk Appetite and Risk Tolerances

One of the more complex aspects of ERM program development is defining the organization's risk appetite and related risk tolerances. As discussed earlier, risk appetite statements are high-level statements that describe the broad levels of risk that the organization's management considers acceptable in pursuit of its strategy and business objectives. Risk tolerances are closely aligned to the organization's business objectives, describe acceptable levels of variation in the risks identified in the risk appetite statements, are narrower in scope, and are more readily measurable and, therefore, actionable. Risk tolerances can be stated as ranges, limits, thresholds, floors, or ceilings and are generally more quantitative in nature.

The following provides examples of risk appetite statements and the corresponding risk tolerances.

Example Risk Appetite and Risk Tolerance Statements

Risk is inherent in the pursuit of our strategy and business objective. These risk appetite and risk tolerance statements embody the standards by which we assume and manage risk.

Risk Categories	*Risk Appetite Examples*	*Risk Tolerance Examples*
Governance and Strategy	We seek new business opportunities that are consistent with our mission, vision, and core values. We strive to anticipate and respond to significant changes in our industry and business. We protect our brand and our culture.	We will pursue new business opportunities that meet the following criteria (explain/list). We will dedicate $X annually to product or service innovation and measure success by (explain). We seek to be relevant in critical client markets (as defined by Y) and grow by X in new/emerging client markets (as defined by Y). We will not introduce new products that do not meet our current standards for X. We will maintain a strong culture of integrity and ethics as measured by our annual employee survey with scores of X or greater.
Regulatory Compliance	We are committed to adhering to the laws and regulations that govern our business. We will not put our business reputation at risk in the pursuit of profit.	No tolerance for regulatory fines, sanctions, or penalties No greater than $X in regulatory settlements per year No tolerance for repeated non-compliance with regulations
People and Talent	We seek to attract, retain, develop, and engage a competent workforce. We maintain a diverse workforce. We strive to ensure safe working conditions for all whom we employ.	Exceed industry employee engagement scores. Diversity targets and ranges of X Employee injury or illness rates of no greater than X U.S. workers comp. loss rate less than X%
Technology and Operations	We seek to meet our clients' expectations for service. We strive to protect our confidential and sensitive data. We seek to avoid significant interruptions to our business operations. We seek to invest in new and emerging technologies. We seek to maintain information security.	Client satisfaction levels no less than X Compliance with customer SLAs (as defined by X) No significant data breaches (as defined by Y) Successful testing of our critical business recovery programs (as defined by X) Successful monitoring of third-party service providers and SLAs (as defined by Y) Acceptable for critical projects No tolerance for information security breaches
Financial	We seek to maintain our strong financial condition. We strive to achieve strong financial results. We prudently invest in new business opportunities.	Leverage or debt/equity ratios, or both, no greater than X; credit ratings of no less than X Operating margins of X% range Risk adjusted return on capital of a minimum X

Linking Current ERM Activities to the ERM Program Plan

Existing ERM activities should be appropriately linked and standardized with the ERM program to be further developed. This initial planning exercise should be enterprise-wide in scope and should be documented, at least at a high level, to support an appropriate review and understanding and to serve as a baseline for program implementation as well as future enhancement.

Documenting ERM Policies

After developing the initial ERM framework, structure, and organization, consideration should be given to documenting other aspects of the ERM program, including the policies and procedures that define and govern the overall ERM process. Such documentation should address all aspects of the ERM program to facilitate ERM program implementation, standardization, communication, and adoption throughout the organization. Such documentation instills discipline and facilitates implementation, and it provides a basis for subsequent program evaluation. Even in smaller organizations, such documentation can be useful in reviews with clients, regulators, lenders, or other authorities who require awareness and evidence of the organization's ERM efforts. The nature and extent of the documentation, however, is a matter of management discretion and should be scaled based upon the size and complexity of the organization.

ERM Program Scalability and Related Considerations

It is important to consider the size and complexity of the organization so that the ERM program can be properly structured, resourced, and scaled. Such consideration will ensure that the organization derives the intended benefits of the program while not burdening the organization with a program that is overly complex or costly. For instance, a larger organization may find that an ERM committee is appropriate, whereas a smaller organization may find that leveraging an existing management committee and integrating ERM into the regular meeting agenda is most efficient. There are many variations for how an ERM program is best resourced and carried out, and an organization is prudent to give such structure and programming the necessary time and consideration in advance.

> "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." (COSO *Enterprise Risk Management—Integrating with Strategy and Performance*, 2017)

ERM Program Technology Considerations

When starting an ERM program, most organizations will find it beneficial to initially use existing technology tools (for example, office shareware, spreadsheets, and templates) for capturing, evaluating, and reporting the organization's enterprise risks. Such technology tools may also be effective in subsequent follow-up and monitoring of risk mitigation and action plans. Once the initial framework is in place, an organization may find it beneficial to adopt more sophisticated technology tools in support of its ERM program. A number of such tools exist. Practitioners may find it helpful to refer to the publications of independent industry observers to obtain an understanding of the current tools available in the market. In addition to considering specific ERM tools, an organization may also find it beneficial to leverage online intranet-based survey tools to gauge employee awareness and perceptions of risk culture and risk attitudes or to obtain information specific to existing or emerging risks.

Suggested outputs from this phase include

- analysis of industry ERM technology tools and practices, and

- a target ERM technology roadmap that defines the current and future technology environment architecture.

The Role of Technology in ERM
"A Real-World Perspective"

Technology can be a key enabler for any risk management program. Most organizations will find that they need a technology solution to manage all of the data gathered, and such solutions may also address monitoring, follow-up, and communication challenges. However, it is important to establish the risk management approach before selecting a technology solution. Otherwise, the organization may be forced to adopt the vendor's approach instead of one that better fits the organization's needs and culture.

Internal Auditing's Role in Risk Management (The IIA Research Foundation, March 2011)

Timeline

The timeline is dependent upon the scope and scale of the organization's targeted ERM program and the sufficiency of project resources, but it typically takes a few weeks to complete this phase.

IV. Gap Analysis

Gap Analysis Phase Objective: The goal of this phase is to compare the organization's current ERM practices against the desired future state, to identify gaps, and to develop actionable recommendations to address these gaps so as to move to the future ERM model.

Now that the organization's current state and desired future state ERM operating model have been established, the organization can identify the gaps that must be filled to implement the future state. These gaps will drive recommendations that can then be prioritized and sequenced into an ERM implementation roadmap. The following are some suggested activities during this phase.

Preliminary Observations

During the gap analysis phase, the project team will begin to develop preliminary observations on gaps and areas for potential improvement. It is important for the team to document these preliminary observations to establish the starting point and provide further analysis. Preliminary observations may consider the following:

- Organization and governance structures supporting ERM and level of engagement by the business with respect to risk management activities
- Processes for strategic planning and determination of risk appetite, risk identification, aggregation, measurement, and reporting of current and future risk
- Communication, escalation, and management of risk issues
- Risk systems, technology, and infrastructure
- Assessment of the current state of the risk management practices
- Current risk processes compared to industry standards and business expectations

The gap analysis should consider all the concepts and components of an effective ERM program to confirm the completeness and accuracy of the information gathered. This approach will help to identify critical gaps in the ERM program, including ERM processes or activities that are not present, adequately designed, implemented, or operating as intended, or those that do not meet the organization's objectives.

The preliminary observations should be socialized or agreed upon, or both, with key stakeholders and further refined and updated.

Recommendations

Once the gap analysis and preliminary observations have been validated, the next step is to develop actionable recommendations to address the identified gaps. These recommendations in turn will facilitate the development of an ERM program implementation roadmap. (The implementation roadmap is addressed in the next phase.)

Suggested outputs from this phase include the following:

- Documented observations on gaps
- Documented recommendations to address identified gaps

Timeline

The timeline for this phase will be dependent upon the extent of the information gathered and the size and nature of the organization's ERM program. This phase is typically a few weeks in duration. If information necessary to complete this phase is difficult to obtain, this phase may be extended.

V. Implementation and Reporting

Implementation and Reporting Phase Objective: The primary goal of this phase is to plan for and implement the targeted ERM operating model or to implement enhancements to an existing ERM program. This phase also includes the implementation or enhancement of the reporting needed to support the implementation as well as the ongoing program.

The implementation phase should consider all the concepts and components of an effective ERM program to ensure completeness of the implemented ERM program. This phase will prioritize aspects of the ERM program as well as plan for and sequence the implementation accordingly. Additionally, to ensure program success, the organization will need to consider appropriate change management activities, including communication and training, to ensure the program's success. During implementation, appropriate information should be reported to measure implementation and program success and to identify any interim program changes or corrections needed to ensure the implemented ERM program is functioning effectively.

Implementation is an important phase for an organization as the ERM team will be validating information from prior phases and putting the operating model into action or revising the existing operating model. Throughout this phase, it is suggested that the ERM team validate results with project sponsors and other interested parties to ensure continued support and that expectations are being appropriately met.

The following are suggested activities in this phase.

Developing Implementation Roadmap and Project Plan

The recommendations developed in the prior phase (Gap Analysis) should now be organized and aggregated into initiatives and/or phases. To build out an implementation plan, these initiatives will need to be sequenced and prioritized. It can be helpful to consider the relative cost and benefits of each initiative to draw insights for appropriate sequencing and prioritization. For example, initiatives that are relatively low in effort and yet will deliver substantial benefits may be prioritized to gain momentum and support for the program.

Additional prioritization considerations include the following:

- Linkages and dependencies between initiatives
- Resource availability
- Project risks, challenges, and other considerations

Once the initiatives are sequenced and prioritized as the basis for the implementation roadmap, a detailed project plan can be created.

Designing Program Performance Measures and Reporting

Implementing or enhancing an ERM program is not a simple or short-term process. It is a long-term commitment, and the organization will benefit from having useful measurements to gauge ongoing progress and success.

Initially, the program performance measures are necessarily focused on the success of the program implementation and, as such, traditional status reports are useful. Post initial implementation, however, ERM program measures and related reporting should be more focused on the quality, timeliness, and effectiveness of the activities as well as the ERM program results and outcomes.

Communication and Training

Effective ERM communication, change management support, and training are crucial to the successful rollout of an ERM program. Throughout program implementation, frequent communication should inform sponsors, employees, and other interested parties (internal and external) about program progress and promote an organization-wide, risk-aware culture. Targeted training should be developed for those more directly involved in the ERM program, including those participating in the event identification and risk assessment process as well as the ongoing ERM monitoring and reporting processes. Communication and training activities should highlight ERM roles and responsibilities and address questions from employees and other interested parties.

Changes to the Implementation Plan

It is not uncommon for issues to arise during the program implementation or shortly after the new or revised ERM operating model has been implemented. The ERM team should be prepared to document issues, investigate causes, resolve issues, and follow-up on program adjustments in response to these issues. To understand the root cause of an issue, the team should ask, "Why, what, and how?" or look for unanticipated changes in variables or assumptions. The following are possible questions to ask during the issue resolution process:

- Why is the ERM program not achieving agreed milestones or objectives?
- How can the ERM program be adapted to get back on track?
- What has changed since the current state was examined or the ERM operating model was designed that could cause implementation challenges?
- What needs to be done to help better train the resources to increase understanding and awareness of the ERM program?

Timeline

The timeline of this phase is dependent upon the scope and scale of the organization's targeted ERM program, the sufficiency of dedicated or available resources, and the extent of technology or other external work required to support the implementation. It is not uncommon for more complex organizations to adopt a phased implementation.

Chapter 5
ERM Program Evaluation and Continuous Improvement

Management should continuously evaluate and monitor the ERM program and make changes to ensure the entire ERM program is functioning effectively. This is best accomplished through ongoing monitoring and separate evaluation activities, such as the following:

- Reports used to monitor operational activities on an ongoing basis may spot inaccuracies or exceptions to anticipated results, including higher rates of incidents or errors.
- Communications from clients, third-party providers, or other external parties might indicate new or emerging issues.
- Regulators, external auditors, and advisors might provide recommendations for improving the ERM program.
- Planning sessions or other meetings may provide important feedback to management on whether the ERM program is effective.

The ERM program should be dynamic because the effectiveness can be affected by a myriad of internal or external changes, including shifts in the organization's strategy to address emerging opportunities, market-related risks, and economic or regulatory conditions affecting the organization. As such, an ERM program must be evaluated to determine whether the program is operating as designed, recent program improvements have been effectively implemented, or the ERM program is keeping pace with change. This evaluation may be part of the organization's periodic review of ERM program effectiveness or may be part of the management activities within a continuous improvement cycle.

I. ERM Program Evaluation

The objective of this activity is to evaluate whether current practices and outcomes are achieving intended benefits. Benefits of this activity include the following:

- **Increasing or enhancing awareness, accountability, and transparency** — A program evaluation can promote better appreciation for and understanding of risk management requirements and responsibilities. An evaluation can also demonstrate management's commitment to maintaining an effective ERM program and help employees better understand the purpose of risk management activities.
- **Evaluating the degree of conformity with the ERM charter, scope, standards, policies, and procedures** — A program evaluation can identify the effectiveness (or failure) of certain steps in the process.
- **Identifying the degree of reliability of risk results and outcomes and related reporting** — Through evaluation, managers at all levels receive information on how effectively risk is being managed and how well existing management efforts and programs are working. In some cases, this information may reveal overlooked or emerging risks or supply new details on existing risks that may prompt changes in risk management approaches.
- **Providing a basis for identifying meaningful program improvement opportunities** — An ERM program evaluation can identify meaningful enhancements and can also measure progress in achieving those improvements.

Approach to an ERM Program Evaluation

An ERM program evaluation can be undertaken post implementation to determine the effectiveness of the new program or after the program has been in place for some time to identify meaningful improvements to

the ERM program. The timing and approach to the evaluation should consider the current maturity of the ERM program to ensure the evaluation is relevant, comprehensive, and provides useful results.

Leveraging the ERM concepts and components (as described in chapter 2) provides meaningful criteria to evaluate the maturity of a current program and to identify areas for improvement. The program evaluation should consider whether the concepts and components are present and, if so, how effectively they are operating at the time of the assessment. Such an evaluation can help an organization assess itself both as of a point in time as well as determine its progress along an ERM maturity continuum over a period of time. An example maturity continuum can be found in appendix B. The Risk Management Society (RIMS) organization also has a helpful tool that can be found online (see additional information in the following box).

The RIMS ERM Program Maturity Model

The RMM is a complimentary, automated tool that can be found online and used to evaluate and score an organization's ERM program (www.rims.org). The tool is organized by core attributes of ERM, which are broken down into success factors and competency or readiness indicators. This helps identify where the ERM program stands on levels of maturity ranging from ad hoc to optimized. It is driven by leading practices from some of the most widely-used risk management standards, including the ISO 31000 and COSO ERM frameworks. The tool can provide a report summarizing an organization's ability to manage risk based on the core attributes and success factors on which the evaluation is based.

II. Continuous Improvement

The implementation of an effective ERM program is not a one-time event. Rather, it requires a continuous process of evolution and refinement. Once the initial implementation of an ERM program has been completed, the organization's risk management program needs to evolve and improve over time to ensure the program continues to be relevant and beneficial. Management plays a critical role in fostering a culture committed to achieving continuous improvement in the organization's ERM program.

Organizations face a wide array of potential sources of change, including both internal (for example, altered objectives and new technologies or processes) and external sources (for example, new competitors, markets, and changes in regulation) that need to be addressed. No matter what source of change, whether it happens over time or occurs suddenly, is incremental or disruptive, or is desired by the organization or forced upon it, organizations cannot ignore these changes and the risks they introduce. As such, an ERM program must seek to anticipate change so that the organization can adapt proactively and avoid becoming obsolete.

Ultimately, there are many benefits that can be derived from continuously improving an ERM program, including the following:

- Facilitating a more informed, risk-based decision-making capability that aligns risk appetite and strategy, effectively allowing management to better meet its strategy and objectives
- Enhancing consistency and communication of the ERM program, which improves opportunities for coordination and understanding between various levels of management and employees throughout the organization
- Fostering a more proactive versus reactive, risk-aware culture and environment
- Ensuring the ongoing effectiveness of the ERM program to sustain organizational success over the long-term

Approach to Continuous Improvement

Continuous improvement can be defined as the structured, ongoing process of identifying and understanding challenges, issues, and opportunities for improvement, and prioritizing and addressing such areas where appropriate. A nimble, successful organization will proactively embrace continuous improvement in its ERM program. Too often, ERM failures occur because organizations were too slow to identify or appropriately react to change or did not react at all. Thus, an ERM program should be treated as a "living" program in which

management and all employees are dedicated to improving the program's levels of performance. Continuous improvement involves good change management techniques for successful implementation.

The process of adapting to change must consider people, processes, systems, and information in a broad sense, and how well its ERM program adapts to change. Often, an organization will conduct a formal, periodic review of its ERM program to evaluate its continued efficacy and capability. Such a review should not, however, be prompted only by a changing environment. Even under seemingly stable conditions, an organization should evaluate its ERM program periodically to consider the continued adequacy of its ERM program capabilities and to look for opportunities for improvement.

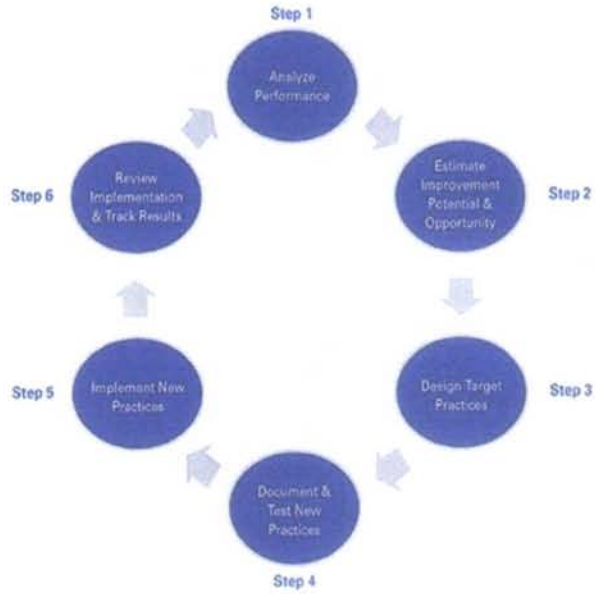
Many organizations have implemented well-known continuous improvement approaches such as Kaizen,[1] Six Sigma,[2] or Lean[3] throughout the organization and may apply these approaches to their ERM program, but having well-known approaches is not mandatory. If an organization is committed to improvement, it can implement its own process.

The following describes a high-level approach to initiating a continuous improvement exercise or program:

- Ensure ERM program documentation is current.
- Evaluate the ERM program versus an ERM maturity framework to identify program gaps or improvement opportunities. Identify, prioritize, and develop initiatives to address program gaps or enhancements.
- Develop a roadmap or plan for completing the initiatives.
- Establish adequate protocols for communicating ERM program evaluation results, initiatives, and plans, including periodic updates to management and the appropriate governing body.

The following illustration shows how an organization might approach a continuous improvement process. This illustration, however, is not a prescriptive example, as the organization's own continuous improvement approach and plan will need to be tailored to meet its specific organizational needs.

Example: Continuous Improvement Approach



[1] Method detailed in Masaaki Imai's book, *Kaizen: The Key to Japan's Competitive Success*. The purpose of continuous improvement is the identification, reduction, and elimination of sub-optimal processes by emphasizing incremental, continual steps.

[2] SixSigma is a set of tools and strategies originally developed by Motorola that became well known after Jack Welch made it a key focus at General Electric. Six Sigma emphasizes continuous efforts from the entire organization for achieving predictable results that can be measured, analyzed, improved, and controlled.

[3] "Lean," first discussed in John Krafcik's article, "Triumph of the Lean Production System," is an approach to identify and eliminate waste and improve quality and "flow" of work.

Point to Consider: An effective ERM leader is a good facilitator and skilled at asking the questions that will support the ongoing effectiveness of ERM and identify areas for improvement such as the following:

- Is there enough dialogue and challenge in our ERM process?
- Do we have enough diversity of thought in our ERM process to ward against bias and challenge our assumptions?
- Do we have active and appropriate engagement at all levels of the organization?

Point to Consider: As an organization becomes more mature and sophisticated in its ERM program, including ongoing and continuous risk and control monitoring, it will likely recognize the need to rely less on ERM processes that are manually-intensive or lack certain beneficial or timely information. These organizations may want to identify and implement systems or tools that automate certain aspects of the ERM program and make them integral to their ongoing operational processes. Such efforts may involve leveraging the organization's existing information or stored data, implementing new information gathering or risk and control systems, or applying more sophisticated analytics or stress-testing to the information gathered.

> "Management leverages and designs its technology to meet a broad range of requirements, including those due to internal and external changes. As organizations respond to changes in the business context in which they operate and adapt their strategy and business objectives, they must also review their technologies." (COSO *Enterprise Risk Management—Integrating with Strategy and Performance*, June 2017).

Commitment to Continuous Improvement

For an ERM program to be successful, an organization should adopt an attitude and culture whereby management is fully committed to the ongoing success and continuous improvement of its ERM program. Both the COSO and ISO risk management frameworks stress that management's commitment at all levels of the organization is foundational to achieving continuous improvement in its ERM capabilities and results.

To ensure the organization's commitment to ERM is genuine, fully embedded in its culture, and sustainable, the organization should define and effectively communicate roles and responsibilities for both achieving an effective ERM program and for continuously improving that program. These roles and responsibilities should consider all levels and activities from the board of directors or equivalent oversight body, to executive management, and other levels of management, as well as other supporting functions, such as legal, compliance internal audit, or other control functions.

The ultimate goal of ERM is to create a "continuous learning organization." By fully involving and engaging all areas of the organization, the organization will ensure its ultimate success not only in achieving the targeted improvements but in ultimately supporting the organization in achieving its objectives.

Glossary of Terms

Please note that some of the terms in this glossary are marked with asterisks (*). One asterisk indicates that the term was taken from COSO Enterprise Risk Management—Integrating with Strategy and Performance; *two asterisks indicate that the term was taken from ISO 31000* Risk Management—Guidelines.

business objectives. Those measurable steps the organization takes to achieve its strategy.*

core values. The organization'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 (ERM). 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.*

external environment. Anything outside of the organization that affects the organization's strategy or its ability to achieve its strategy and business objectives.

external stakeholders. Any stakeholders who are not considered internal to the organization (for example, shareholders, donors, benefactors, governmental agencies, or regulators).

ERM 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.*

ERM process. A series of actions or steps taken, which are integral to an ERM program and are described by the expected ERM core components. This publication describes these core components by leveraging the COSO ERM framework's eight interrelated components.

ERM program. The end-to-end set of activities that allows an organization to operationalize and fully execute its ERM process. A program includes governance, people, processes and systems, and ongoing management and continuous improvement.

event. An occurrence or set of occurrences.*

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 organization's strategy or business objectives.*

inherent risk. The risk to an organization in the absence of any actions management might take to alter either the risk's likelihood or impact.

internal control. A process, effected by an organization's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.*

internal environment. Anything inside of the organization that influences its strategy or its ability to achieve its strategy and business objectives.

likelihood. The possibility that a given event will occur.*

mission. The organization's core purpose, which establishes what it wants to accomplish and why it exists.*

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

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

portfolio view. A composite view of risk the organization faces, which positions management and the board to consider both an enterprise view of risk, as well as interdependencies of the risks and how they may affect the organization's performance relative to its strategy and business objectives.

reasonable expectation. The amount of risk of achieving strategy and business objectives that is appropriate for an organization, recognizing that no one can predict risk with precision.*

residual risk. The remaining risk after management has applied controls and/or has otherwise taken action to alter the risk's likelihood or impact.

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

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

risk appetite statement. The written statement or documentation of an organization's risk appetite.

risk assessment. Overall process of risk identification, risk analysis, and risk evaluation.

risk capacity. The maximum amount of risk that an organization is able to absorb in the pursuit of strategy and business objectives.*

risk identification. Process of finding, recognizing, and describing risks that might help or prevent an organization achieving its objectives.

risk impact. The possible effect of an event.

risk inventory. A comprehensive listing of risks, stated in standardized terms, often using a risk taxonomy. Sometimes referred to as a risk register.

risk management. Coordinated activities to direct and control an organization with regard to risk.**

risk management philosophy. The set of shared beliefs and attitudes characterizing how the organization considers risk in everything it does, from strategy development and implementation to its day-to-day activities.

risk profile. A composite view of the risk assumed at a particular level of the organization, 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.*

risk response. Selected actions to manage identified risks including avoiding, accepting, reducing, or sharing risk.

risk taxonomy. A common set of risk categories, definitions, or terms used to help describe, identify, and communicate risks.

risk tolerance. The acceptable level of variation relative to the achievement of a specific objective, often best measured in the same units as those used to measure the related objective.

risk treatment. Process of selecting and implementing a risk response or options for addressing risk.

risk velocity. How quickly the risk impact could potentially follow the onset of the risk.

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 organization.*

strategic objectives. An organization's high-level goals, aligned with and supporting its mission/vision, reflecting management's choice as to how the organization will seek to create value for its stakeholders.

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 organization's aspirations for its future state or what the organization aims to achieve over time.*

Appendix A
COSO and ISO 31000 Framework Mapping

The matrix in this appendix is a summary comparison of the elements found in the COSO ERM framework and the ISO 31000 framework and is referenced periodically in this publication. If the ISO 31000 framework includes similar concepts to the COSO ERM framework, cross-references to the specific section of the ISO 31000 framework are included in the following table.

COSO ERM Components and Principles	*ISO 31000 Framework—Elements*
1.0 Governance and Culture	
Principle 1: Exercises Board Risk Oversight *The board of directors provides oversight of the strategy and carries out governance responsibility to support management in achieving strategy and business objectives.*	See ISO 31000, *Risk Management—Guidelines*, section 5.2, "Leadership and commitment." See ISO 31000, *Risk Management—Guidelines*, section 5.4.3, "Assigning organizational roles, authorities, responsibilities and accountabilities."
Topics covered include the following: • **Accountability and Responsibility** • **Skills, Expertise, and Business Knowledge** • **Independence** • **Suitability of Enterprise Risk Management** • **Organizational Bias**	
Principle 2: Establishes Operating Structures *The organization establishes operating structures in the pursuit of strategy and business objectives.*	See ISO 31000, *Risk Management—Guidelines*, section 5.2, "Leadership and commitment." See ISO 31000, *Risk Management—Guidelines*, section 5.3, "Integration." See ISO 31000, *Risk Management—Guidelines*, section 5.4.3, "Assigning organizational roles, authorities, responsibilities and accountabilities."
Topics covered include the following: • **Operating Structure and Reporting Lines** • **Enterprise Risk Management Structure** • **Authority and Responsibilities** • **Enterprise Risk Management within the Evolving Organization**	
Principle 3: Defines Desired Culture *The organization defines the desired behaviors that characterize the organization's desired culture.*	See ISO 31000, *Risk Management—Guidelines*, section 5.4.1, "Understanding the organization and its context."

(continued)

COSO ERM Components and Principles	*ISO 31000 Framework—Elements*
Topics covered include the following: • **Culture and Desired Behaviors** • **Applying Judgment** • **Effect of Culture** • **Aligning Core Values, Decision-Making, and Behavior** • **Shifting Culture**	
Principle 4: Demonstrates Commitment to Core Values *The organization demonstrates a commitment to the organization's core values.*	See ISO 31000, *Risk Management—Guidelines*, section 5.2, "Leadership and commitment." See ISO 31000, *Risk Management—Guidelines*, section 5.4.2, "Articulating risk management commitment." See ISO 31000, *Risk Management—Guidelines*, section 5.4.3, "Assigning organizational roles, authorities, responsibilities and accountabilities." See ISO 31000, *Risk Management—Guidelines*, section 5.4.5, "Establishing communication and consultation." See ISO 31000, *Risk Management—Guidelines*, section 6.2, "Communication and consultation."
Topics covered include the following: • **Reflecting Core Values throughout the Organization** • **Embracing a Risk-Aware Culture** • **Enforcing Accountability** • **Holding Itself Accountable** • **Keeping Communication Open and Free from Retribution** • **Responding to Deviations in Core Values and Behaviors**	
Principle 5: Attracts, Develops, and Retains Capable Individuals *The organization is committed to building human capital in alignment with the strategy and business objectives.*	See ISO 31000, *Risk Management—Guidelines*, section 5.4.4, "Allocating resources."
Topics covered include the following: • **Establishing and Evaluating Competence** • **Attracting, Developing and Retaining Individuals** • **Rewarding Performance** • **Addressing Pressure** • **Preparing for Succession**	
2.0 Strategy and Objective Setting	
Principle 6: Analyzes Business Context *The organization considers the potential effects of business context on the risk profile.*	See ISO 31000, *Risk Management—Guidelines*, section 5.4.1, "Understanding the organization and its context." See ISO 31000, *Risk Management—Guidelines*, section 6.3.3, "External and internal context."

COSO ERM Components and Principles	*ISO 31000 Framework—Elements*
Topics covered include the following: • Understanding Business Context • Considering External Environment and Stakeholders • Considering Internal Environment and Stakeholders • How Business Context Affects Risk Profile	
Principle 7: Defines Risk Appetite *The organization defines risk appetite in context of creating, preserving, and realizing value.*	
Topics covered include the following: • Applying Risk Appetite • Determining Risk Appetite • Articulating Risk Appetite • Using Risk Appetite	
Principle 8: Evaluates Alternative Strategies *The organization evaluates alternative strategies and the potential impact on risk profile.*	
Topics covered include the following: • The Importance of Aligning Strategy • Understanding the Implications from Chosen Strategy • Aligning Strategy with Risk Appetite • Making Changes to Strategy • Mitigating Bias	
Principle 9: Formulates Business Objectives *The organization considers risk while establishing the business objectives at various levels that align and support strategy.*	
Topics covered include the following: • Establish Business Objectives • Aligning Business Objectives • Understanding the Implications from Chosen Business Objectives • Categorizing Business Objectives • Setting Performance Measures and Targets • Understanding Tolerances • Performance Measures and Established Tolerances	
3.0 Performance	
Principle 10: Identifies Risk *The organization identifies risks that affect the performance of strategy and business objectives.*	See ISO 31000, *Risk Management—Guidelines*, section 6.4.2, "Risk identification."

(continued)

COSO ERM Components and Principles	*ISO 31000 Framework—Elements*
Topics covered include the following: • Identifying Risk • Using a Risk Inventory • Approaches to Identifying Risk • Framing Risk	
Principle 11: Assesses Severity of Risk *The organization assesses the severity of risk.*	See ISO 31000, *Risk Management—Guidelines*, section 6.4.3, "Risk analysis."
Topics covered include the following: • Assessing Risk • Selecting Severity Measures • Assessment Approaches • Inherent, Target, and Residual Risk • Depicting Assessment Results • Identifying Triggers for Reassessment • Bias in Assessment	
Principle 12: Prioritizes Risk *The organization prioritizes risks as a basis for selecting responses to risks.*	See ISO 31000, *Risk Management—Guidelines*, section 6.4.4, "Risk evaluation."
Topics covered include the following: • Establishing the Criteria • Prioritizing Risk • Using Risk Appetite to Prioritize Risk • Prioritization at All Levels • Bias in Prioritization	
Principle 13: Implements Risk Responses *The organization identifies and selects risk responses.*	See ISO 31000, *Risk Management—Guidelines*, section 6.5.1, "Selection of risk treatment options." See ISO 31000, *Risk Management—Guidelines*, section 6.5.3, "Preparing and implementing risk treatment plans."
Topics covered include the following: • Choosing Risk Responses • Selecting and Deploying Risk Responses • Considering Costs and Benefits of Risk Responses • Additional Considerations	
Principle 14: Develops Portfolio View *The organization develops and evaluates a portfolio view of risk.*	
Topics covered include the following: • Understanding a Portfolio View • Developing a Portfolio View • Analyzing the Portfolio View	

COSO ERM Components and Principles	*ISO 31000 Framework—Elements*
4.0 Review and Revision	
Principle 15: Assesses Substantial Change *The organization identifies and assesses changes that may substantially affect strategy and business objectives.*	See ISO 31000, *Risk Management—Guidelines*, section 5.6, "Evaluation." See ISO 31000, *Risk Management—Guidelines*, section 5.7.1, "Adapting." See ISO 31000, *Risk Management—Guidelines*, section 5.7.2, "Continually improving." See ISO 31000, *Risk Management—Guidelines*, section 6.6, "Monitoring and review."
Topics covered include the following: • **Integrating Reviews into Business Practices** • **Internal Environment** • **External Environment**	
Principle 16: Reviews Risk and Performance *The organization reviews organization performance results and considers risk.*	See ISO 31000, *Risk Management—Guidelines*, section 6.6, "Monitoring and review."
Topics covered include the following: • **Integrating Reviews into Business Practices** • **Considering Organization Capabilities**	
Principle 17: Pursues Improvement in Enterprise Risk Management *The organization pursues improvement of enterprise risk management.*	See ISO 31000, *Risk Management—Guidelines*, section 6.6, "Monitoring and review." See ISO 31000, *Risk Management—Guidelines*, section 5.7.1, "Adapting." See ISO 31000, *Risk Management—Guidelines*, section 5.7.2, "Continually improving."
Topics covered include the following: • **Pursuing Improvement**	
5.0 Information, Communication, and Reporting	
Principle 18: Leverages Information and Technology *The organization leverages the organization's information systems to support enterprise risk management.*	
Topics covered include the following: • **Putting Relevant Information to Use** • **Evolving Information** • **Data Sources** • **Categorizing Risk Information** • **Managing Data** • **Using Technology to Support Information** • **Changing Requirements**	

(continued)

COSO ERM Components and Principles	*ISO 31000 Framework—Elements*
Principle 19: Communicates Risk Information *The organization uses communication channels to support enterprise risk management.*	See ISO 31000, *Risk Management—Guidelines*, section 6.2, "Communication and consultation." See ISO 31000, *Risk Management—Guidelines*, section 6.7, "Recording and reporting."
Topics covered include the following: • **Communicating with Stakeholders** • **Communicating with the Board** • **Methods of Communicating**	
Principle 20: Reports on Risk, Culture, and Performance *The organization reports on risk culture and performance at multiple levels and across the organization.*	See ISO 31000, *Risk Management—Guidelines*, section 6.2, "Communication and consultation." See ISO 31000, *Risk Management—Guidelines*, section 6.7, "Recording and reporting."
Topics covered include the following: • **Identifying Report Users and Their Roles** • **Reporting Attributes** • **Types of Reporting** • **Reporting Risks to the Board** • **Reporting on Culture** • **Key Indicators** • **Reporting Frequency and Quality**	

Appendix B
Example ERM Program Maturity Self-Assessment

The following matrix can be used to evaluate the current state of an ERM program. This matrix provides criteria or attributes for evaluating the maturity of the ERM program across the COSO ERM components and principles (as described in the "III. Components of an ERM Program" section of chapter 2).

After evaluating the individual ERM program components and principles, the matrix can also be used to provide an overall rating of the program, although considerable judgment will be needed to make such a determination as a typical ERM program will not be uniform in its maturity across the components. The ultimate goal, however, is to provide a baseline to determine the specific actions that can be taken to mature the ERM program and to track outcomes and improvements as compared to the baseline. The overall rating will be used primarily for purposes of creating an awareness of the current state, garnering support for making targeted improvements, and communicating results. Thus, although not an exact measurement, determining the overall rating is still a helpful exercise.

> "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." (COSO *Enterprise Risk Management—Integrating with Strategy and Performance*, 2017)

ERM Program Maturity Matrix

ERM Maturity Levels	1. Ad-Hoc	2. Defined	3. Systematic	4. Integrated
ERM Program Components	*No standard framework or formal process or program for ERM exists. Risk management is ad-hoc and primarily reactive.*	*An initial ERM process and program have been defined but are not completely or consistently in place or implementation is in process.*	*An ERM process and program have been consistently implemented across the organization and are operating as designed.*	*The ERM program includes all systematic elements of an ERM program; ERM processes are fully embedded in strategy setting and business management practices and an ongoing improvement process is in place.*

(continued)

ERM Program Maturity Matrix—*continued*

ERM Maturity Levels	1. Ad-Hoc	2. Defined	3. Systematic	4. Integrated
1.0 Governance and Culture **Exercises Board Risk Oversight** **Establishes Operating Structures** **Defines Desired Culture** **Demonstrates Commitment to Core Values** **Attracts, Develops, and Retains Capable Individuals**	• Little explicit board emphasis or oversight of risk • No formal risk structure or leadership for risk management or implementation • No formal articulation of risk culture or risk management expectations • No formal risk communication or training available	• Board oversight is defined, and reporting is in place. • Risk leadership and ownership are established. • Operating and reporting lines are established to carry out risk management objectives. • Management articulates and communicates the organization's risk culture and commitment to core values. • Programs are in place to attract, develop, and retain capable individuals.	• Board oversight is well established and there is evidence of board review and challenge. • Formal risk governance structure, charter, policies, and procedures are in place, are well understood, and functioning as designed. • Management emphasizes the importance of risk management and having a risk-aware culture (that is, actively supports an appropriate "tone at the top"). • The organization hires (or has access to) capable individuals with relevant experience who can exercise judgment and oversight in accordance with their responsibilities. • Ongoing risk communications are in place and risk management training is required for all employees.	• Board oversight is well established and there is evidence of ongoing oversight, review, and challenge, particularly in strategy setting. • A process is in place to continuously assess and improve the effectiveness of risk governance, structure, process, and program. • Management continuously communicates the organization's core values and its expectations for maintaining a risk-aware culture. Risk culture and awareness are measured and programs are in place to continuously improve outcomes. • Awareness and responsibility for risks are evenly distributed across the operating structure (everyone is a "risk manager"). • Risk management responsibilities, capabilities, and accountabilities are included in employee performance expectations and reviews. • Management strives to continuously develop and improve risk awareness and risk management capabilities throughout the organization.

ERM Program Maturity Matrix—*continued*

ERM Maturity Levels	1. Ad-Hoc	2. Defined	3. Systematic	4. Integrated
2.0 Strategy and Objective Setting Analyzes Business Context Defines Risk Appetite Evaluates Alternative Strategies Formulates Business Objectives	• Risk appetite is not formally documented, leveraged, or shared • No clear relationship exists between organization's strategy and business objectives and its risk appetite	• Risk appetite is established, communicated, and shared. • Management considers risk appetite when setting strategy and business objectives.	• A comprehensive risk appetite and related risk tolerances are defined, communicated, and measured. • Risk appetite informs strategy and business objectives setting to maximize outcomes. • A process is in place to incorporate risk appetite in decision-making and to measure performance within established risk appetite tolerances or ranges.	• Consideration of risk appetite and the organization's risk profile are critical to strategy and business objective setting. • Risk appetite informs ongoing decision-making. • Business performance is routinely compared to risk appetite and risk tolerances to ensure actual performance is in line with targeted outcomes or to inform resulting actions.
3.0 Performance Identifies Risk Assesses Severity of Risk Prioritizes Risks Implements Risk Responses Develops Portfolio View	• No formal risk identification and assessment standards or process exist • Risk assessments, prioritization, and response activities performed on an ad-hoc or case-by-case basis without formal or standard process • Risks evaluated only after an adverse event has occurred • Unexpected positive outcomes not analyzed • No formal or enterprise-wide reporting or analysis of risk	• A standard risk identification, assessment, and prioritization of risk process has been established and is performed at least annually. • A portfolio view of prioritized risk exists. • Risk responses are identified, implemented, and tracked.	• Robust risk identification, assessment, and prioritization processes are well-established across the organization and are timely to appropriately consider new and emerging risks. • A portfolio view of prioritized risks exists, and risk interdependencies are identified and analyzed to understand impact to risk profile. • Risk prioritization considers risk appetite and risk prioritization results are considered in determining risk responses to optimize resource allocations.	• Enterprise-wide performance activities are critical management activities that contribute to the achievement of strategy and business objectives. • A portfolio view of risks allows management to stress test its risk profile and maximize its opportunities and outcomes. • Management seeks to continuously improve upon its ERM performance capabilities and outcomes. • Risk response includes the development and testing of a crisis management plan.

(continued)

ERM Program Maturity Matrix—*continued*

ERM Maturity Levels	1. Ad-Hoc	2. Defined	3. Systematic	4. Integrated
4.0 Review and Revision **Assesses Substantial Change** **Reviews Risk and Performance** **Pursues Improvement in Enterprise Risk Management**	• Organization does not have formal processes for identifying changes that affect business strategy or objectives or the risks affecting performance	• The organization has developed a process for identifying internal/external changes that affect strategy and business objectives and for reviewing risks to organization performance. • The organization is in the process of implementing or improving its existing ERM program.	• The organization has a process for identifying and responding to internal/external changes affecting its strategy and business objectives. • The organization has a well-functioning process for evaluating the impact of risk on its achievement of its strategy and objectives and to respond accordingly. • The organization has a process for identifying and implementing enhancements to its ERM program.	• The organization considers how internal/external change affects not only business performance but also the underlying key assumptions used to develop business strategy and business objectives to better inform future strategy and business objective setting. • The organization leverages the results of its risk and performance review to reduce variations in performance, revise its existing strategy and/or business objectives, or to identify new opportunities. • The organization has a robust continuous improvement program focused on improving its ERM program and outcomes.

ERM Program Maturity Matrix—*continued*

ERM Maturity Levels	1. Ad-Hoc	2. Defined	3. Systematic	4. Integrated
5.0 Information, Communication, and Reporting **Leverages Information and Technology** **Communicates Risk Information** **Reports on Risk, Culture, and Performance**	• Reporting primarily supports external reporting or regulatory compliance requirements • Risk information is not readily available, communicated, or shared across the organization • Risk information gathering is ad hoc, decentralized, and/or manual in nature	• Standard risk reporting and communication is in place. • Readily available information and/or information systems support the ERM process.	• Qualitative and quantitative ERM reporting exists to cover all aspects of the ERM process and outcomes. • Risks are formally and timely communicated and escalated to management and the board. • Risk information systems have been developed and deployed across the organization.	• Emphasis is placed on capturing, reporting, and analyzing forward-looking risk indicators. • Efficient and effective information systems support all aspects of the ERM program and process. • Reporting also includes measures and monitors of risk awareness and culture. • Programs are in place to continuously improve information communication and reporting.

Appendix C
References

In developing this publication, the following ERM frameworks, standards, and guides were referenced:

- COSO *Enterprise Risk Management—Integrating with Strategy and Performance*, June 2017.
- The ISO 31000 *Risk Management—Guidelines*, February 2018.
- The Institute of Internal Auditors Position Paper, "The Role of Internal Auditing in Enterprise-wide Risk Management," January 2009.
- RIMS Risk Maturity Model (RMM). Accessed May 2014. www.rims.org.

ID 19 1002 2382
ISBN 9781948306362

APAERM18P

AICPA & CIMA

Worldwide leaders in public and management accounting

aicpa.org | AICPAStore.com