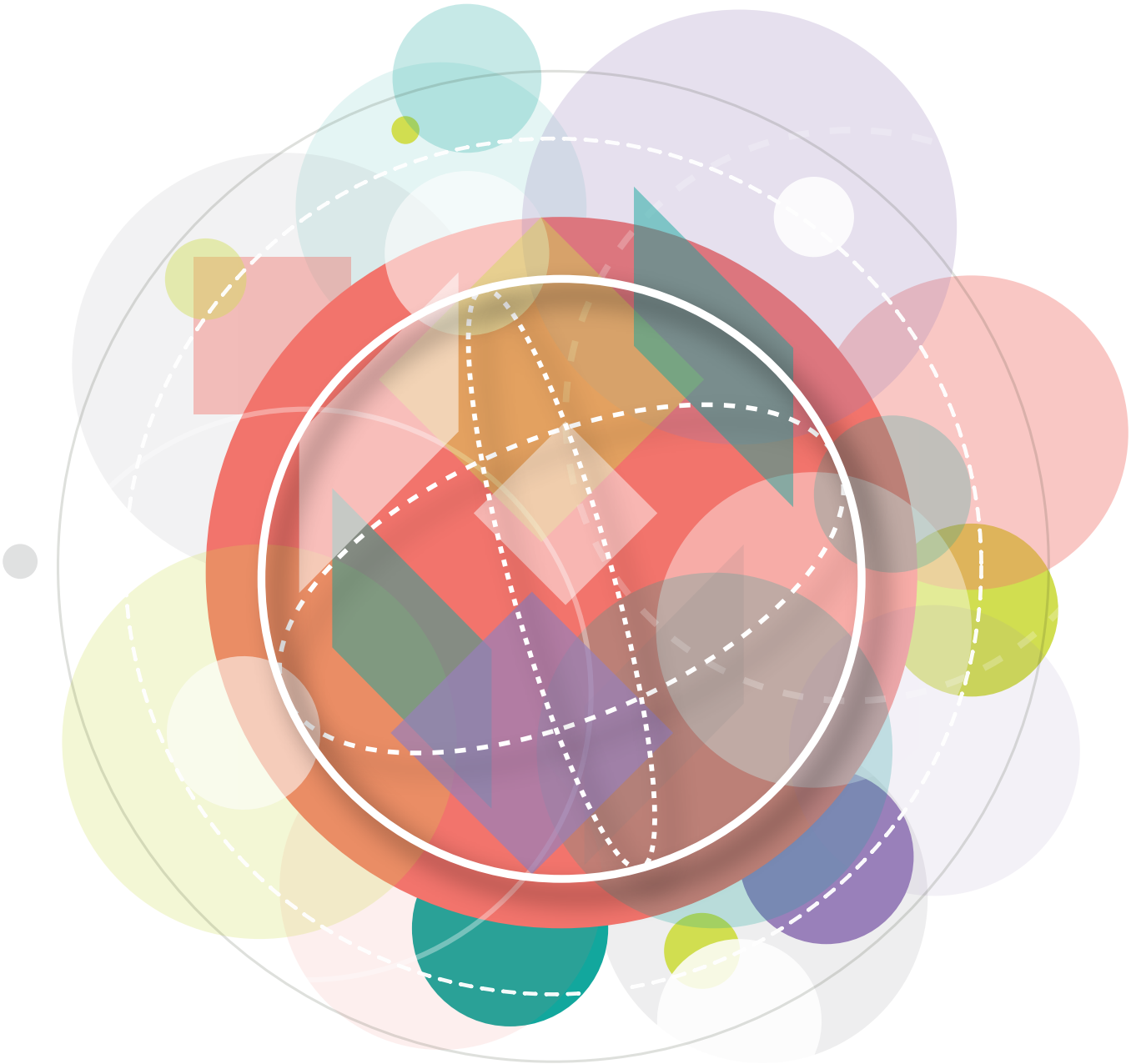
COSO

Committee of Sponsoring Organizations of the Treadway Commission

Enterprise Risk Management

Integrating with Strategy and Performance

Executive Summary



June 2017

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

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

Foreword

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

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

- Provides greater insight into the value of enterprise risk management when setting and carrying out strategy.
- Enhances alignment between performance and enterprise risk management to improve the setting of performance targets and understanding the impact of risk on performance.
- Accommodates expectations for governance and oversight.
- Recognizes the globalization of markets and operations and the need to apply a common, albeit tailored, approach across geographies.
- Presents new ways to view risk to setting and achieving objectives in the context of greater business complexity.
- Expands reporting to address expectations for greater stakeholder transparency.
- Accommodates evolving technologies and the proliferation of data and analytics in supporting decision-making.
- Sets out core definitions, components, and principles for all levels of management involved in designing, implementing, and conducting enterprise risk management practices.

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

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

Robert B. Hirth Jr.
COSO Chair

Dennis L. Chesley
PwC Project Lead Partner and Global and APA Risk and Regulatory Leader

Committee of Sponsoring Organizations of the Treadway Commission

Board Members

Robert B. Hirth Jr.
COSO Chair

Richard F. Chambers
The Institute of Internal Auditors

Mitchell A. Danaher
Financial Executives International

Charles E. Landes
American Institute of Certified Public Accountants

Douglas F. Prawitt
American Accounting Association

Sandra Richtermeyer
Institute of Management Accountants

PwC—Author

Principal Contributors

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

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

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

Matthew Bagin
Director
Washington DC, USA

Hélène Katz
Director
New York, USA

Katie T. Sylvis
Director
Washington DC, USA

Sallie Jo Perraglia
Manager
New York, USA

Kathleen Crader Zelnik
Manager
Washington DC, USA

Maria Grimshaw
Senior Associate
New York, USA

The Changing Risk Landscape

Our understanding of the nature of risk, the art and science of choice, lies at the core of our modern economy. Every choice we make in the pursuit of objectives has its risks. From day-to-day operational decisions to the fundamental trade-offs in the boardroom, dealing with risk in these choices is a part of decision-making.

As we seek to optimize a range of possible outcomes, decisions are rarely binary, with a right and wrong answer. That's why enterprise risk management may be called both an art and a science. And when risk is considered in the formulation of an organization's strategy and business objectives, enterprise risk management helps to optimize outcomes.

Our understanding of risk and our practice of enterprise risk management have improved greatly over the past few decades. But the margin for error is shrinking. The World Economic Forum has commented on the "increasing volatility, complexity and ambiguity of the world."[1] That's a phenomenon we all recognize. Organizations encounter challenges that impact reliability, relevancy, and trust. Stakeholders are more engaged today, seeking greater transparency and accountability for managing the impact of risk while also critically evaluating leadership's ability to crystalize opportunities. Even success can bring with it additional downside risk—the risk of not being able to fulfill unexpectedly high demand, or maintain expected business momentum, for example.

Organizations need to be more adaptive to change. They need to think strategically about how to manage the increasing volatility, complexity, and ambiguity of the world, particularly at the senior levels in the organization and in the boardroom where the stakes are highest.

Enterprise Risk Management—Integrating with Strategy and Performance provides a Framework for boards and management in entities of all sizes. It builds on the current level of risk management that exists in the normal course of business. Further, it demonstrates how integrating enterprise risk management practices throughout an entity helps to accelerate growth and enhance performance. It also contains principles that can be applied—from strategic decision-making through to performance.

Below, we describe why it makes sense for management and boards to use the enterprise risk management framework,[2] what organizations have achieved by applying enterprise risk management, and what further benefits they can realize through its continued use. We conclude with a look into the future.

Management's Guide to Enterprise Risk Management

Management holds overall responsibility for managing risk to the entity, but it is important for management to go further: to enhance the conversation with the board and stakeholders about using enterprise risk management to gain a competitive advantage. That starts by deploying enterprise risk management capabilities as part of selecting and refining a strategy.

Most notably, through this process, management will gain a better understanding of how the explicit consideration of risk may impact the choice of strategy. Enterprise risk management enriches management dialogue by adding perspective to the strengths and weaknesses of a strategy as conditions change, and to how well a strategy fits with the organization's mission and vision. It allows management to feel more confident that they've examined alternative strategies and considered the input of those in their organization who will implement the strategy selected.

1 The Global Risks Report 2016, 11th edition, World Economic Forum (2016).

2 The Framework uses the term "board of directors" or "board," which encompasses the governing body, including board, supervisory board, board of trustees, general partners, or owner.

Once strategy is set, enterprise risk management provides an effective way for management to fulfill its role, knowing that the organization is attuned to risks that can impact strategy and is managing them well. Applying enterprise risk management helps to create trust and instill confidence in stakeholders in the current environment, which demands greater scrutiny than ever before about how risk is actively addressing and managing these risks.

The Board's Guide to Enterprise Risk Management

Every board has an oversight role, helping to support the creation of value in an entity and prevent its decline. Traditionally, enterprise risk management has played a strong supporting role at the board level. Now, boards are increasingly expected to provide oversight of enterprise risk management.

The Framework supplies important considerations for boards in defining and addressing their risk oversight responsibilities. These considerations include governance and culture; strategy and objective-setting; performance; information, communications and reporting; and the review and revision of practices to enhance entity performance.

The board's risk oversight role may include, but is not limited to:

- Reviewing, challenging, and concurring with management on:
  - Proposed strategy and risk appetite.
  - Alignment of strategy and business objectives with the entity's stated mission, vision, and core values
  - Significant business decisions including mergers acquisitions, capital allocations, funding, and dividend-related decisions
  - Response to significant fluctuations in entity performance or the portfolio view of risk.
  - Responses to instances of deviation from core values.
- Approving management incentives and remuneration.
- Participating in investor and stakeholder relations.

Over the longer term, enterprise risk management can also enhance enterprise resilience—the ability to anticipate and respond to change. It helps organizations identify factors that represent not just risk, but change, and how that change could impact performance and necessitate a shift in strategy. By seeing change more clearly, an organization can fashion its own plan; for example, should it defensively pull back or invest in a new business? Enterprise risk management provides the right framework for boards to assess risk and embrace a mindset of resilience.

Questions for management

Can all of management—not just the chief risk officer—articulate how risk is considered in the selection of strategy or business decisions? Can they clearly articulate the entity's risk appetite and how it might influence a specific decision? The resulting conversation may shed light on what the mindset for risk taking is really like in the organization.

Boards can also ask senior management to talk not only about risk processes but also about culture. How does the culture enable or inhibit responsible risk taking? What lens does management use to monitor the risk culture, and how has that changed? As things change—and things will change whether or not they're on the entity's radar—how can the board be confident of an appropriate and timely response from management?

What Enterprise Risk Management Has Achieved

COSO published *Enterprise Risk Management—Integrated Framework* in 2004. The purpose of that publication was to help entities better protect and enhance stakeholder value. Its underlying philosophy was that "value is maximized when management sets strategy and objectives to strike an optimal balance between growth and return goals and related risks, and efficiently and effectively deploys resources in pursuit of the entity's objectives."[3]

[3] *Enterprise Risk Management—Integrated Framework*, Executive Summary, COSO (2004).

Since its publication, the *Framework* has been used successfully around the world, across industries, and in organizations of all types and sizes to identify risks, manage those risks within a defined risk appetite, and support the achievement of objectives. Yet, while many have applied the *Framework* in practice, it has the potential to be used more extensively. It would benefit from examining certain aspects with more depth and clarity, and by providing greater insight into the links between strategy, risk, and performance. In response, therefore, the updated Framework in this publication:

- More clearly connects enterprise risk management with a multitude of stakeholder expectations.
- Positions risk in the context of an organization's performance, rather than as the subject of an isolated exercise.
- Enables organizations to better anticipate risk so they can get ahead of it, with an understanding that change creates opportunities, not simply the potential for crises.

This update also answers the call for a stronger emphasis on how enterprise risk management informs strategy and its performance.

Benefits of Effective Enterprise Risk Management

All organizations need to set strategy and periodically adjust it, always staying aware of both ever-changing opportunities for creating value and the challenges that will occur in pursuit of that value. To do that, they need the best possible framework for optimizing strategy and performance.

That's where enterprise risk management comes into play. Organizations that integrate enterprise risk management throughout the entity can realize many benefits, including, though not limited to:

- *Increasing the range of opportunities:* By considering all possibilities—both positive and negative aspects of risk—management can identify new opportunities and unique challenges associated with current opportunities.
- *Identifying and managing risk entity-wide:* Every entity faces myriad risks that can affect many parts of the organization. Sometimes a risk can originate in one part of the entity but impact a different part. Consequently, management identifies and manages these entity-wide risks to sustain and improve performance.
- *Increasing positive outcomes and advantage while reducing negative surprises:* Enterprise risk management allows entities to improve their ability to identify risks and establish appropriate responses, reducing surprises and related costs or losses, while profiting from advantageous developments.

Clearing up a few misconceptions

We've heard a few misconceptions about the original *Framework* since it was introduced in 2004. To set the record straight:

Enterprise risk management is not a function or department. It is the culture, capabilities, and practices that organizations integrate with strategy-setting and apply when they carry out that strategy, with a purpose of managing risk in creating, preserving, and realizing value.

Enterprise risk management is more than a risk listing. It requires more than taking an inventory of all the risks within the organization. It is broader and includes practices that management puts in place to actively manage risk.

Enterprise risk management addresses more than internal control. It also addresses other topics such as strategy-setting, governance, communicating with stakeholders, and measuring performance. Its principles apply at all levels of the organization and across all functions.

Enterprise risk management is not a checklist. It is a set of principles on which processes can be built or integrated for a particular organization, and it is a system of monitoring, learning, and improving performance.

Enterprise risk management can be used by organizations of any size. If an organization has a mission, a strategy, and objectives—and the need to make decisions that fully consider risk—then enterprise risk management can be applied. It can and should be used by all kinds of organizations, from small businesses to community-based social enterprises to government agencies to Fortune 500 companies.

- *Reducing performance variability:* For some, the challenge is less with surprises and losses and more with variability in performance. Performing ahead of schedule or beyond expectations may cause as much concern as performing short of scheduling and expectations. Enterprise risk management allows organizations to anticipate the risks that would affect performance and enable them to put in place the actions needed to minimize disruption and maximize opportunity.
- *Improving resource deployment:* Every risk could be considered a request for resources. Obtaining robust information on risk allows management, in the face of finite resources, to assess overall resource needs, prioritize resource deployment and enhance resource allocation.
- *Enhancing enterprise resilience:* An entity's medium- and long-term viability depends on its ability to anticipate and respond to change, not only to survive but also to evolve and thrive. This is, in part, enabled by effective enterprise risk management. It becomes increasingly important as the pace of change accelerates and business complexity increases.

These benefits highlight the fact that risk should not be viewed solely as a potential constraint or challenge to setting and carrying out a strategy. Rather, the change that underlies risk and the organizational responses to risk give rise to strategic opportunities and key differentiating capabilities.

The Role of Risk in Strategy Selection

Strategy selection is about making choices and accepting trade-offs. So it makes sense to apply enterprise risk management to strategy as that is the best approach for untangling the art and science of making well-informed choices.

Risk is a consideration in many strategy-setting processes. But risk is often evaluated primarily in relation to its potential effect on an already-determined strategy. In other words, the discussions focus on risks to the existing strategy: We have a strategy in place, what could affect the relevance and viability of our strategy?

But there are other questions to ask about strategy, which organizations are getting better at asking: Have we modeled customer demand accurately? Will our supply chain deliver on time and on budget? Will new competitors emerge? Is our technology infrastructure up to the task? These are the kinds of questions that executives grapple with every day, and responding to them is fundamental to carrying out a strategy.

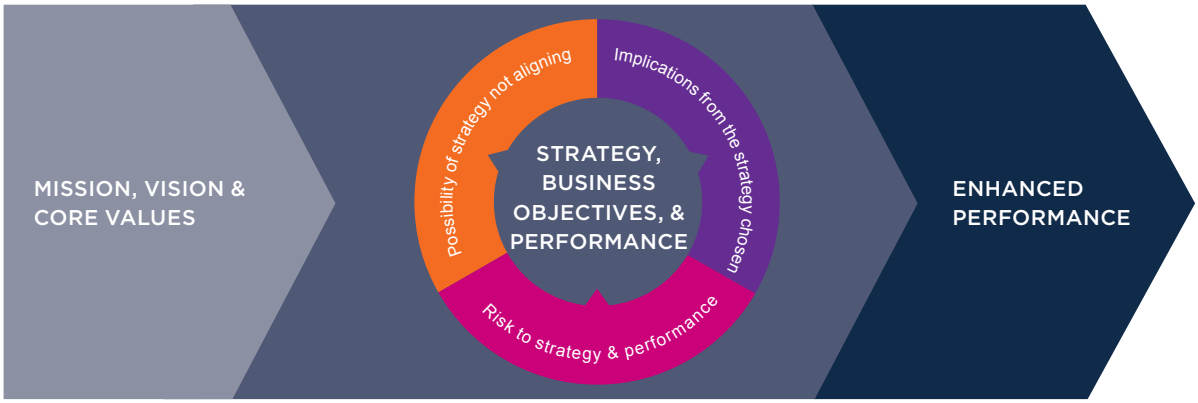
However, the risk to the chosen strategy is only one aspect to consider. As this Framework emphasizes, there are two additional aspects to enterprise risk management that can have far greater effect on an entity's value: the possibility of the strategy not aligning, and the implications from the strategy chosen.

The first of these, **the possibility of the strategy not aligning with an organization's mission, vision, and core values**, is central to decisions that underlie strategy selection. Every entity has a mission, vision, and core values that define what it is trying to achieve and how it wants to conduct business. Some organizations are skeptical about truly embracing their corporate credos. But mission, vision, and core values have been demonstrated to matter—and they matter most when it comes to managing risk and remaining resilient during periods of change.

A chosen strategy must support the organization's mission and vision. A misaligned strategy increases the possibility that the organization may not realize its mission and vision, or may compromise its values, even if a strategy is successfully carried out. Therefore, enterprise risk management considers the possibility of strategy not aligning with the mission and vision of the organization.

The other additional aspect is **the implications from the strategy chosen**. When management develops a strategy and works through alternatives with the board, they make decisions on the trade-offs inherent in the strategy. Each alternative strategy has its own risk profile—these are the implications arising from the strategy. The board of directors and management need to determine if the strategy works in tandem with the organization's risk appetite, and how it will help drive the organization to set objectives and ultimately allocate resources efficiently.

Here's what's important: Enterprise risk management is as much about understanding the *implications from the strategy and the possibility of strategy not aligning* as it is about managing risks to set objectives. The figure below illustrates these considerations in the context of mission, vision, core values, and as a driver of an entity's overall direction and performance.



Enterprise risk management, as it has typically been practiced, has helped many organizations identify, assess, and manage risks to the strategy. But the most significant causes of value destruction are embedded in the possibility of the strategy not supporting the entity's mission and vision, and the implications from the strategy.

Enterprise risk management enhances strategy selection. Choosing a strategy calls for structured decision-making that analyzes risk and aligns resources with the mission and vision of the organization.

A Focused Framework

Enterprise Risk Management—Integrating with Strategy and Performance clarifies the importance of enterprise risk management in strategic planning and embedding it throughout an organization—because risk influences and aligns strategy and performance across all departments and functions.

The Framework itself is a set of principles organized into five interrelated components:

1. **Governance and Culture**: Governance sets the organization's tone, reinforcing the importance of, and establishing oversight responsibilities for, enterprise risk management. Culture pertains to ethical values, desired behaviors, and understanding of risk in the entity.
2. **Strategy and Objective-Setting**: Enterprise risk management, strategy, and objective-setting work together in the strategic-planning process. A risk appetite is established and aligned with strategy; business objectives put strategy into practice while serving as a basis for identifying, assessing, and responding to risk.
3. **Performance**: Risks that may impact the achievement of strategy and business objectives need to be identified and assessed. Risks are prioritized by severity in the context of risk appetite. The organization then selects risk responses and takes a portfolio view of the amount of risk it has assumed. The results of this process are reported to key risk stakeholders.
4. **Review and Revision**: By reviewing entity performance, an organization can consider how well the enterprise risk management components are functioning over time and in light of substantial changes, and what revisions are needed.
5. **Information, Communication, and Reporting**: Enterprise risk management requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across the organization.

The five components in the updated Framework are supported by a set of principles.[4] These principles cover everything from governance to monitoring. They're manageable in size, and they describe practices that can be applied in different ways for different organizations regardless of size, type, or sector. Adhering to these principles can provide management and the board with a reasonable expectation that the organization understands and strives to manage the risks associated with its strategy and business objectives.

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

Looking into the Future

There is no doubt that organizations will continue to face a future full of volatility, complexity, and ambiguity. Enterprise risk management will be an important part of how an organization manages and prospers through these times. Regardless of the type and size of an entity, strategies need to stay true to their mission. And all entities need to exhibit traits that drive an effective response to change, including agile decision-making, the ability to respond in a cohesive manner, and the adaptive capacity to pivot and reposition while maintaining high levels of trust among stakeholders.

As we look into the future, there are several trends that will have an effect on enterprise risk management. Just four of these are:

- *Dealing with the proliferation of data:* As more and more data becomes available and the speed at which new data can be analyzed increases, enterprise risk management will need to adapt. The data will come from both inside and outside the entity, and it will be structured in new ways. Advanced analytics and data visualization tools will evolve and be very helpful in understanding risk and its impact—both positive and negative.
- *Leveraging artificial intelligence and automation:* Many people feel that we have entered the era of automated processes and artificial intelligence. Regardless of individual beliefs, it is important for enterprise risk management practices to consider the impact of these and future technologies, and leverage their capabilities. Previously unrecognizable relationships, trends and patterns can be uncovered, providing a rich source of information critical to managing risk.
- *Managing the cost of risk management:* A frequent concern expressed by many business executives is the cost of risk management, compliance processes, and control activities in comparison to the value gained. As enterprise risk management practices evolve, it will become important that activities spanning risk, compliance, control, and even governance be efficiently coordinated to provide maximum benefit to the organization. This may represent one of the best opportunities for enterprise risk management to redefine its importance to the organization.

[4] A fuller description of these twenty principles is provided at the end of this document.

- *Building stronger organizations:* As organizations become better at integrating enterprise risk management with strategy and performance, an opportunity to strengthen resilience will present itself. By knowing the risks that will have the greatest impact on the entity, organizations can use enterprise risk management to help put in place capabilities that allow them to act early. This will open up new opportunities.

In summary, enterprise risk management will need to change and adapt to the future to consistently provide the benefits outlined in the Framework. With the right focus, the benefits derived from enterprise risk management will far outweigh the investments and provide organizations with confidence in their ability to handle the future.

Acknowledgments

A special thank you to the following companies and organizations for allowing the participation of Advisory Council Members and Observers.

Advisory Council Members

Companies and Organizations

- Athene USA (Jane Karli)
- Edison International (David J. Heller)
- First Data Corporation (Lee Marks)
- Georgia-Pacific LLC (Paul Sobel)
- Invesco Ltd. (Suzanne Christensen)
- Microsoft (Jeff Pratt)
- US Department of Commerce (Karen Hardy)
- United Technologies Corporation (Margaret Boissoneau)
- Zurich Insurance Company (James Davenport)

Higher Education and Associations

- North Carolina State University (Mark Beasley)
- St. John's University (Paul Walker)
- The Institute of Internal Auditors (Douglas J. Anderson)

Professional Service Firms

- Crowe Horwath LLP (William Watts)
- Deloitte & Touche LLP (Henry Ristuccia)
- Ernst & Young (Anthony J. Carmello)
- James Lam & Associates (James Lam)
- Grant Thornton LLP (Bailey Jordan)
- KPMG LLP Americas (Deon Minnaar)
- Mercury Business Advisors Inc. (Patrick Stroh)
- Protiviti Inc. (James DeLoach)

Former COSO Board Member

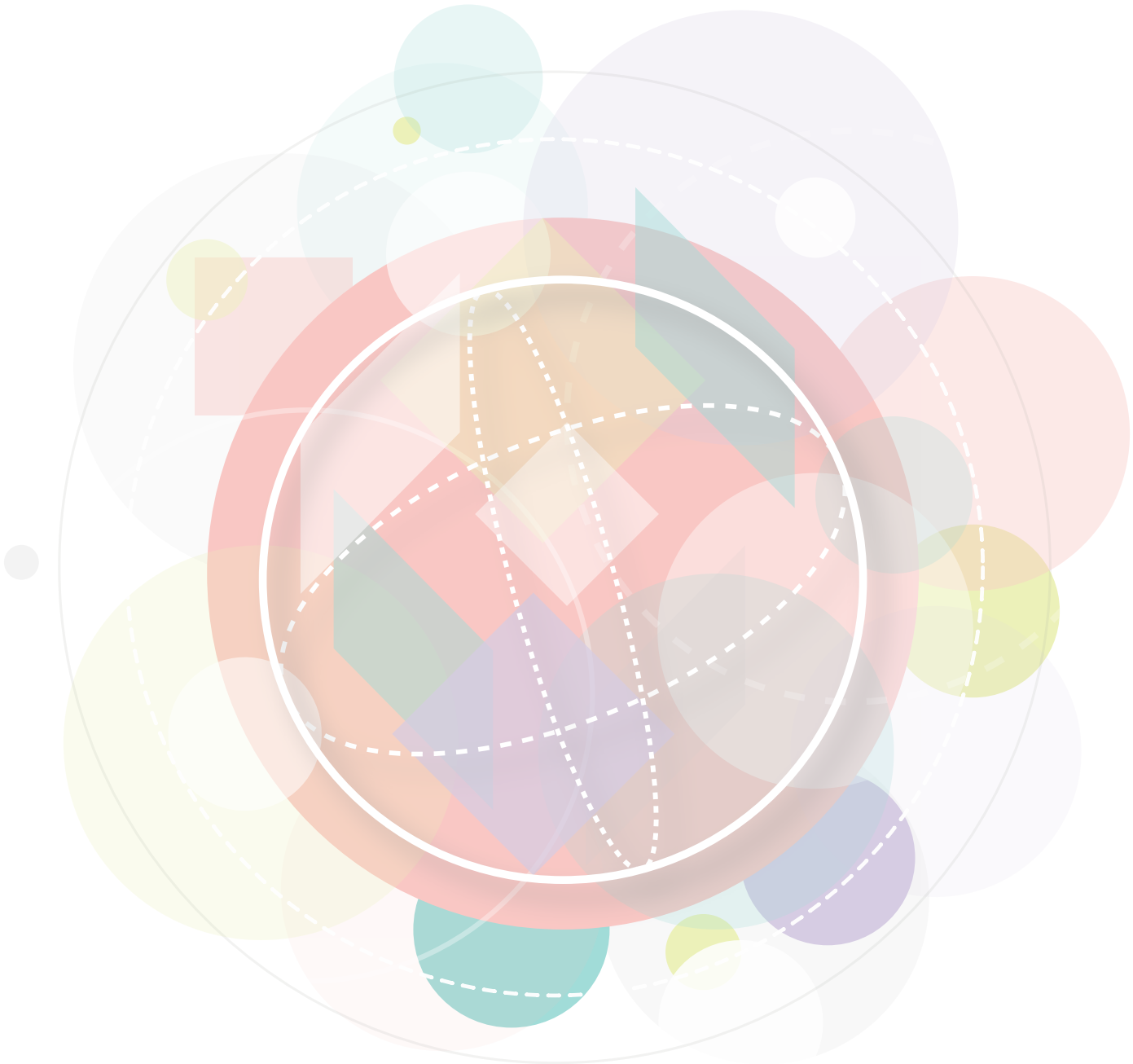
- COSO Chair, 2009–2013 (David Landsittel)

Observers

- Federal Deposit Insurance Corporation (Harrison Greene)
- Government Accountability Office (James Dalkin)
- Institute of Management Accountants (Jeff Thompson)
- Institut der Wirtschaftsprüfer (Horst Kreisel)
- International Federation of Accountants (Vincent Tophoff)
- ISACA (Jennifer Bayuk)
- Risk Management Society (Carol Fox)

Components and Principles

1. **Exercises Board Risk Oversight**—The board of directors provides oversight of the strategy and carries out governance responsibilities to support management in achieving strategy and business objectives.
2. **Establishes Operating Structures**—The organization establishes operating structures in the pursuit of strategy and business objectives.
3. **Defines Desired Culture**—The organization defines the desired behaviors that characterize the entity's desired culture.
4. **Demonstrates Commitment to Core Values**—The organization demonstrates a commitment to the entity's core values.
5. **Attracts, Develops, and Retains Capable Individuals**—The organization is committed to building human capital in alignment with the strategy and business objectives.
6. **Analyzes Business Context**—The organization considers potential effects of business context on risk profile.
7. **Defines Risk Appetite**—The organization defines risk appetite in the context of creating, preserving, and realizing value.
8. **Evaluates Alternative Strategies**—The organization evaluates alternative strategies and potential impact on risk profile.
9. **Formulates Business Objectives**—The organization considers risk while establishing the business objectives at various levels that align and support strategy.
10. **Identifies Risk**—The organization identifies risk that impacts the performance of strategy and business objectives.
11. **Assesses Severity of Risk**—The organization assesses the severity of risk.
12. **Prioritizes Risks**—The organization prioritizes risks as a basis for selecting responses to risks.
13. **Implements Risk Responses**—The organization identifies and selects risk responses.
14. **Develops Portfolio View**—The organization develops and evaluates a portfolio view of risk.
15. **Assesses Substantial Change**—The organization identifies and assesses changes that may substantially affect strategy and business objectives.
16. **Reviews Risk and Performance**—The organization reviews entity performance and considers risk.
17. **Pursues Improvement in Enterprise Risk Management**—The organization pursues improvement of enterprise risk management.
18. **Leverages Information Systems**—The organization leverages the entity's information and technology systems to support enterprise risk management.
19. **Communicates Risk Information**—The organization uses communication channels to support enterprise risk management.
20. **Reports on Risk, Culture, and Performance**—The organization reports on risk, culture, and performance at multiple levels and across the entity.



A full version of *Enterprise Risk Management—Integrating with Strategy and Performance* can be purchased by visiting the www.coso.org website.