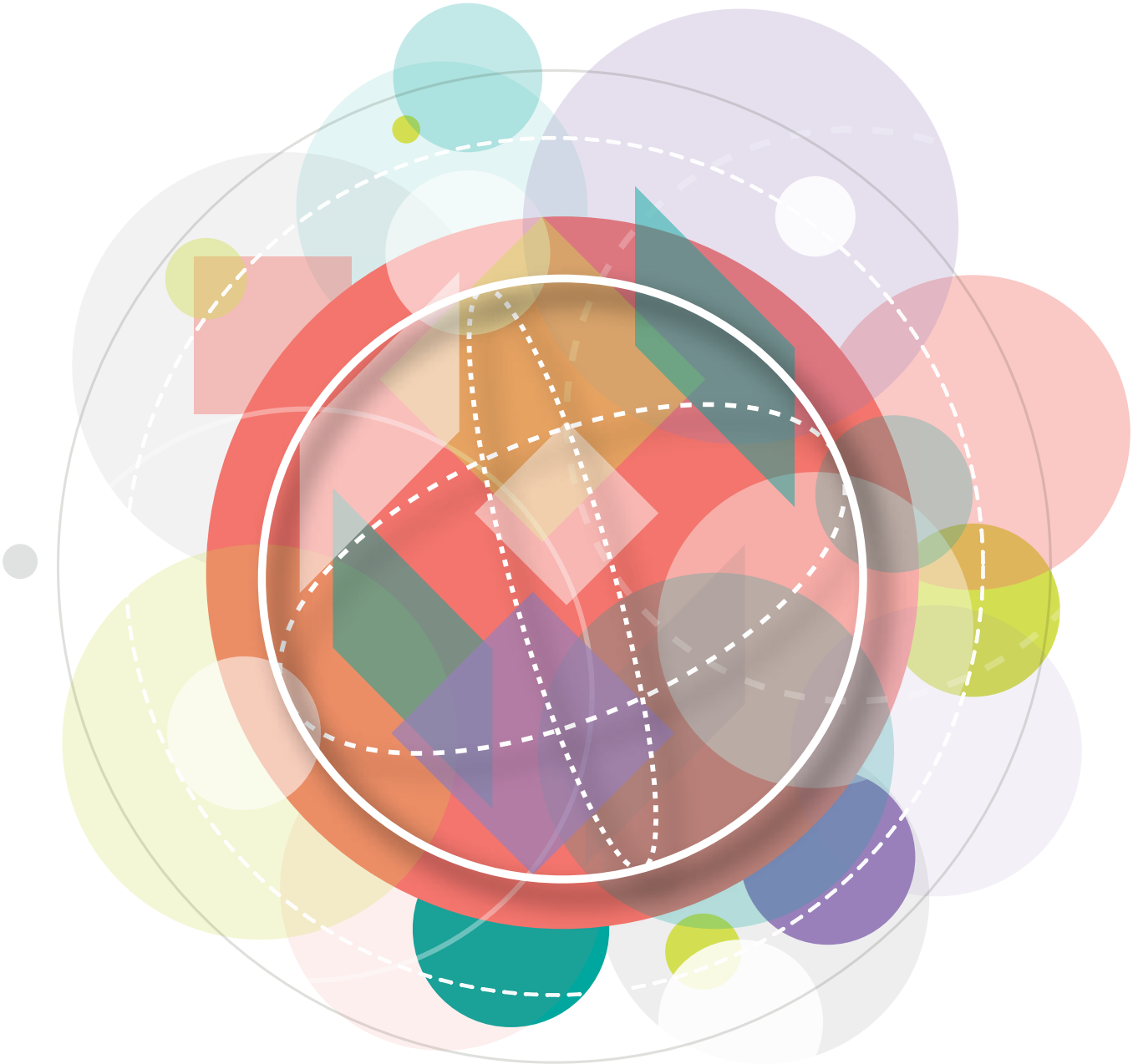
Committee of Sponsoring Organizations of the Treadway Commission

Enterprise Risk Management

Aligning Risk with Strategy and Performance

Executive Summary



June 2016 edition

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 boards have enhanced their awareness and oversight of enterprise risk management while asking for improved risk reporting. This update to the 2004 publication addresses the evolution of enterprise risk management and the need for organizations to improve their approach to managing risk in today's business environment.

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

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

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

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

The COSO Board would like to thank PwC for its significant contributions in developing *Enterprise Risk Management—Aligning Risk 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
Global Risk 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 US Advisory Leader
New York, USA

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

Frank J. Martens
Project Lead Director
Vancouver, Canada

Matthew Bagin
Director
Washington DC, USA

Hélène Katz
Director
New York, USA

Sallie Jo Perraglia
Manager
New York, USA

Kate T. Sylvis
Manager
McLean Virginia, USA

Kathleen Crader Zelnik
Manager
Washington DC, USA

Maria Grimshaw
Senior Associate
New York, USA

The Changing Risk Landscape

1. 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 the day-to-day operational decisions to the fundamental trade-offs in the boardroom, dealing with uncertainty in these choices is a part of decision-making.
2. As we seek to optimize a range of uncertain 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 uncertainty is considered in the formulation of an organization's strategy and business objectives, enterprise risk management helps to optimize outcomes.
3. 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 writes of the "increasing volatility, complexity and ambiguity of the world."[1] That's a phenomenon we all recognize. Organizations find challenges impacting reliability, relevancy, and trust. Stakeholders are more engaged today, seeking greater transparency and accountability for managing risk. Even success can bring with it risk—the risk of not being able to fulfill unexpectedly high demand or the ability to maintain business momentum that has become an expectation, for example.
4. Organizations need to become 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.
5. *Enterprise Risk Management—Aligning Risk with Strategy and Performance* includes a Framework for boards and management in organizations of all sizes. It demonstrates how integrating enterprise risk management into an organization helps to accelerate growth and enhance performance by more closely linking strategy and objectives to both risk and opportunity. The Framework contains principles they can apply—from strategic decision-making through to execution. Integrating enterprise risk management throughout an entity provides a clear path to creating, preserving, and realizing value.
6. Below, we describe why the enterprise risk management framework makes sense for use by senior management and in the boardroom, what enterprise risk management has achieved, and how it can do more to inform and help shape strategy and improve decision-making.

The Board's Guide to Enterprise Risk Management

7. The board of directors[2] has a risk oversight responsibility, and its mix of skills, experience, and business knowledge need to be appropriate to assess risk in light of the business's strategy and objectives. All boards need to satisfy themselves that enterprise risk management practices are consistent with the entity's[3] strategy and risk appetite, and that a culture of risk-aware decision-making is embedded throughout the organization.
8. Boards have an opportunity, however, to go further: to use enterprise risk management to enhance the conversation with management and stakeholders. Enterprise risk

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.

3 This Executive Summary uses the term "entity" when referring to any form of for-profit company, not-for-profit organization, or government body.

management—one of the best frameworks available for decision-making in the face of uncertainty—should be deployed as part of the critical process of selecting and refining a strategy.

9. Most notably, boards gain a better understanding of how risk may impact the choice of strategy. Enterprise risk management enriches boardroom dialogue by providing a comprehensive sense of a strategy's strengths and weaknesses as conditions change, and of a strategy's fit with the organization's mission. Directors can feel more confident that they've looked at alternative strategies with a critical eye and can have a more robust discussion with management.

10. Once strategy is set, enterprise risk management provides an effective way for a board to fulfill its risk oversight role by knowing that the organization is attuned to risks that can impact strategy and is managing them well. Boards are under greater scrutiny than ever before about how they oversee risk. They need to create trust and instill confidence in their stakeholders—many of whom are growing louder in demanding accountability and transparency. Enterprise risk management is one more step toward fulfilling their responsibility.

What Enterprise Risk Management Has Achieved

11. COSO published *Enterprise Risk Management—Integrated Framework* in 2004. Its philosophy was to help entities better protect and enhance stakeholder value: "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."[4] Since then, the *Framework* has been used successfully around the world and 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.

12. Yet, as we've seen the *Framework* applied in practice, we've recognized that it has the potential to be used more extensively. We realized that certain aspects would benefit from more depth and clarity, as well as greater insight into the links between strategy, risk, and performance. Therefore, the updated Framework in the current 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.

4 *Enterprise Risk Management—Integrated Framework*, Executive Summary, COSO (2004).

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 more than a risk listing. Managing risk across an organization requires more than listing the "top 10" risks or making an inventory of all risks within the organization. Enterprise risk management is broader and includes practices that management puts in place to actively manage risk to appropriate levels.

Enterprise risk management addresses more than internal control. Internal control is an integral subset of enterprise risk management. But enterprise risk management also addresses other topics such as setting strategy, 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 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 under uncertainty—then enterprise risk management can be applied. Enterprise risk management can and should be applied by all kinds of organizations, from small shops to community-based social enterprises to government agencies to Fortune 500 companies.

- Enables organizations to become more anticipatory so they can get ahead of risk. Organizations in this position understand that change creates valuable opportunities, not simply the potential for crises.

13. This update also answers the call for a stronger emphasis on enterprise risk management when informing strategy and its execution.

The Strategic Value of the COSO Framework

14. All organizations need to set and periodically adjust strategy with an awareness of both ever-changing opportunities for creating value and—at the same time—the challenges they will face in pursuit of that value. They need the best possible framework for optimizing strategy and performance.

15. That's where enterprise risk management—defined as *the culture, capabilities, and practices, integrated with strategy and execution, that organizations rely on to manage risk in creating, preserving, and realizing value*—comes into play. Organizations that integrate enterprise risk management can obtain a range of 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.
    - *Reducing negative surprises and increasing gains*: 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.
    - *Reducing performance variability*: For some, the challenge is less with surprises and losses and more with variability in performance. In addition, performing ahead of schedule or beyond expectations may cause as much concern as performing short of scheduling and expectations. Enterprise risk management allows entities to anticipate the risks that would impact performance and enable them to put in place the actions needed to minimize disruption.
    - *Improving resource deployment*: Obtaining robust information on risk allows management to assess overall resource needs and enhance resource allocation.

16. Further, 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. That capability is called "enterprise resilience," and it is increasingly important as the business environment becomes more uncertain and the pace of change accelerates. Fortune 500 companies with multiple business units and loyal customers cannot easily "pivot" their strategies in the face of change the way smaller organizations can. Regardless of size, strategies need to stay true to their mission. And all organizations 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.

17. These benefits highlight the fact that risk should not be viewed solely as a potential constraint or challenge to executing a strategy. Rather, the change that underlies risk and the organizational responses to risk also give rise to strategic opportunities and key differentiating capabilities. As such, the role of risk in selecting and evaluating a strategy requires deeper consideration.

The Role of Risk in Strategy Selection

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

19. 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 strategy: "We have a strategy in place, what could affect the relevance and viability of our strategy?"

20. Organizations are getting better at asking the right questions and putting practices in place to deal with those kinds of risks. 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 that are fundamental to executing a strategy.

21. However, risk to the chosen strategy is only one aspect of risk 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 overall risk profile.

22. Central to decisions that underlie selection of a strategy, the second aspect is the possibility of strategy not aligning with an organization's mission, vision, and core values. 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 are skeptical about organizations 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.

23. 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 executed. Therefore, enterprise risk management considers the possibility of strategy not aligning with the mission and vision of the organization.

24. Then there is a third aspect. 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 from the strategy. The board of directors and management need to consider how 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.

25. Additionally, alternative strategies are built on different assumptions, and those assumptions are sensitive to change in different ways. Change may come in the form of rates of innovation, customer behaviors, shifting employee capabilities, competitive responses, regulatory shifts, geopolitical developments—or just about any other factor that upends the assumptions behind a strategy. Boards should want to understand these sensitivities—the implications from the strategy—before they approve a strategy. They should also monitor business developments to ascertain whether these assumptions continue to remain valid, and if not, what actions need to be taken, including revisiting strategy.

26. 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 creating an inventory of all risks within the organization. These considerations are why enterprise risk management, as depicted below, can be so valuable in the strategy-setting process.

27. Enterprise risk management, as it has typically been practiced, has helped many organizations identify, manage, and mitigate 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. Analyses of underperforming organizations reveal that they lost their way because of strategic blunders (*possibility of* and *implications from*), rather than operational errors, compliance faults, or external events (*risks to*).

28. Enterprise risk management helps to make the evaluation of strategy rooted in the decisions made by senior management much clearer. It clarifies how strategy selection can be enhanced. Choosing a strategy calls for structured decision-making that analyzes risk and aligns budgets and activities with the mission and vision of the organization.

Aligning Risk with Strategy and Performance

29. *Enterprise Risk Management—Aligning Risk with Strategy and Performance* clarifies the importance of enterprise risk management's role in strategic planning and demonstrates that it is more easily embedded throughout an organization—because risk influences and aligns strategy and performance across all departments and functions.

30. The Framework itself is a set of principles organized in five interrelated components:

    1. **Risk Governance and Culture:** Risk 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.

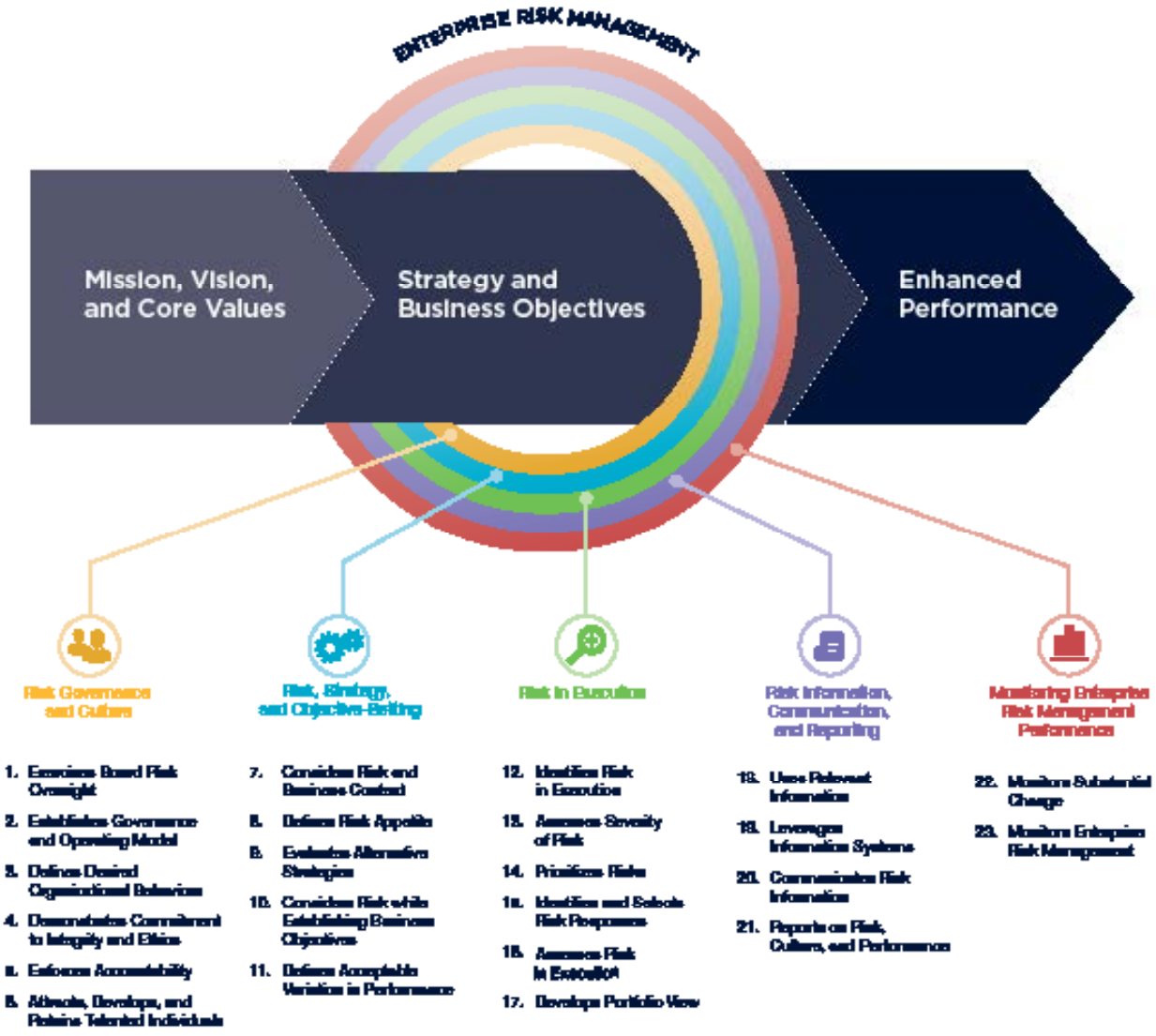
    2. **Risk, Strategy, and Objective-Setting:** Enterprise risk management, strategy, and objective-setting work together in the strategic-planning process. A risk appetite is established and aligned with strategy; business objectives put strategy into practice while serving as a basis for identifying, assessing, and responding to risk.

    3. **Risk in Execution:** 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. **Risk 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.

5. **Monitoring Enterprise Risk Management Performance:** By monitoring risk management performance, an organization can consider how well the enterprise risk management components are functioning over time and in light of substantial changes.

31. There are 23 principles, noted below, that support the five components.[5] 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 or sector. Adhering to these principles can provide a reasonable expectation to management and the board that the organization understands and is able to manage the risks associated with the strategy and business objectives to an acceptable level.



5 A fuller description of these 23 principles is provided on the inside back cover.

Looking Forward

32. Enterprise risk management helps boards do their job better. Every board has an oversight role, helping to prevent the destruction of value. Traditionally, enterprise risk management has played a strong supporting role. Now, boards are increasingly expected to contribute to value creation through oversight and involvement in vetting strategy. *Enterprise Risk Management—Aligning Risk with Strategy and Performance* makes the connection clearer.

33. An important way that directors fulfill their responsibilities is through probing dialogue that not only tests assumptions but also draws out insights into strategy selection and ultimately enables better decisions. Specifically, boards should consider asking different kinds of questions about risk and resilience to their leadership in order to enhance the dialogue with management to include the more strategic aspects of enterprise risk management.

34. For example, can the leaders in entities—not just the chief risk officer—articulate how risk factors into 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.

35. Boards can also ask senior management to talk not only about risk processes but also about risk culture. How does the culture enable or inhibit responsible risk taking? What lens does management use to monitor the company's 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?

36. 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 and objectives. 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 that mindset of resilience.

Acknowledgments

37. 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 (Cynthia Armine-Klein)
- 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 (Doug 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)

23 principles

1. **Exercises Board Risk Oversight**—The board of directors provides oversight of the strategy and carries out risk governance responsibilities to support management in achieving strategy and business objectives.
2. **Establishes Governance and Operating Model**—The organization establishes governance and operating structures in the pursuit of strategy and business objectives.
3. **Defines Desired Organizational Behaviors**—The organization defines the desired behaviors that characterize the entity's core values and attitudes toward risk.
4. **Demonstrates Commitment to Integrity and Ethics**—The organization demonstrates a commitment to integrity and ethical values.
5. **Enforces Accountability**—The organization holds individuals at all levels accountable for enterprise risk management, and holds itself accountable for providing standards and guidance.
6. **Attracts, Develops, and Retains Talented Individuals**—The organization is committed to building human capital in alignment with the strategy and business objectives.
7. **Considers Risk and Business Context**—The organization considers potential effects of business context on risk profile.
8. **Defines Risk Appetite**—The organization defines risk appetite in the context of creating, preserving, and realizing value.
9. **Evaluates Alternative Strategies**—The organization evaluates alternative strategies and impact on risk profile.
10. **Considers Risk while Establishing Business Objectives**—The organization considers risk while establishing the business objectives at various levels that align and support strategy.
11. **Defines Acceptable Variation in Performance**—The organization defines acceptable variation in performance relating to strategy and business objectives.
12. **Identifies Risk in Execution**—The organization identifies risk in execution that impacts the achievement of business objectives.
13. **Assesses Severity of Risk**—The organization assesses the severity of risk.
14. **Prioritizes Risks**—The organization prioritizes risks as a basis for selecting responses to risks.
15. **Identifies and Selects Risk Responses**—The organization identifies and selects risk responses.
16. **Assesses Risk in Execution**—The organization assesses operating performance results and considers risk.
17. **Develops Portfolio View**—The organization develops and evaluates a portfolio view of risk.
18. **Uses Relevant Information**—The organization uses information that supports enterprise risk management.
19. **Leverages Information Systems**—The organization leverages the entity's information systems to support enterprise risk management.
20. **Communicates Risk Information**—The organization uses communication channels to support enterprise risk management.
21. **Reports on Risk, Culture, and Performance**—The organization reports on risk, culture, and performance at multiple levels of and across the entity.
22. **Monitoring Substantial Change**—The organization identifies and assesses internal and external changes that may substantially impact strategy and business objectives.
23. **Monitors Enterprise Risk Management**—The organization monitors enterprise risk management performance.

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