COSO

Committee of Sponsoring Organizations of the Treadway Commission

Enterprise Risk Management

Aligning Risk with Strategy and Performance

Frequently Asked Questions

November 2016 edition

COSO Enterprise Risk Management – Aligning Risk with Strategy and Performance

Public Exposure – Frequently Asked Questions

Table of Contents

Project Background

Why update the 2004 Enterprise Risk Management–Integrated Framework?

In October 2014, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) announced a project to review and update the 2004 *Enterprise Risk Management–Integrated Framework* (*Framework*). The *Framework* is widely accepted and used by management and boards to enhance an organization's ability to manage uncertainty and to consider how much risk to accept as they strive to increase stakeholder value.

Since 2004, the complexity of risk has changed, significant new risks have emerged, and boards have enhanced their awareness and oversight of risk management while asking for improved risk reporting. Updates to the *Framework* reflect current and evolving concepts and applications of enterprise risk management, so that organizations worldwide can attain better value from enterprise risk management. Specifically, it provides greater insight into strategy and the role of enterprise risk management in the setting and execution of strategy, enhances the alignment between organizational performance and enterprise risk management, and accommodates expectations for governance and oversight.

What documents are being updated?

The 2004 *Enterprise Risk Management-Integrated Framework: Executive Summary* and *Framework* are both being updated. The *Updated Document* is titled the *Enterprise Risk Management – Aligning Risk with Strategy and Performance*. This *Updated Document* consists of two sections. The first section offers a perspective on current and evolving concepts and applications of enterprise risk management. The second section of the document, the Framework, accommodates different viewpoints and organizational structures, and enhances the consideration of risk in the selection and execution of strategies and decision-making. With this updated structure, the new document is referred to as the *Updated Document*.

Are there any documents from 2004 not being updated?

Yes, the volume of *Application Techniques* which provided illustrations of techniques used at various levels of an organization in applying enterprise risk management components will not be updated as part of this project.

What approach is COSO using to update the original Framework?

The PwC Project Team, with COSO Board oversight, has and will continue to carefully consider the merits of feedback and opinions throughout the project. To do so, the PwC Project Team reviews and embraces input that helps in the development of a relevant, logical, and internally consistent document in all phases of the project. These phases include:

- *Assess and Envision* – Through literature reviews, global surveys, public roundtables, and forums, this phase identified current challenges for organizations implementing enterprise risk management. During this phase, PwC analyzed information, reviewed various sources of input, and identified critical issues and concerns. COSO launched a global survey, available to the general public, for providing input on the original *Framework*, soliciting almost 900 responses.
- *Build and Design* – PwC, with COSO Board oversight, developed the *Updated Document*, which was reviewed by the COSO Advisory Council and Observers to gather reactions and suggestions.
- *Public Exposure* – With assistance provided by the Advisory Council and oversight of the COSO Board, PwC prepared exposure drafts and an on-line questionnaire to facilitate a review by the general public.
- *Finalization* – PwC will analyze all comments received and refine the documents for needed modifications. The COSO Board and Advisory Council will also consider whether the *Updated Document* is sound, logical, and useful to management of entities of all types and sizes. PwC will finalize the *Updated Document* and provide the update to the COSO Board for review and acceptance.

COSO Enterprise Risk Management – Aligning Risk with Strategy and Performance

Public Exposure – Frequently Asked Questions

Project Governance

Who is COSO?

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a joint initiative of five private sector organizations: The American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), the Institute of Internal Auditors (IIA), and the Institute of Management Accountants (IMA). COSO provides thought leadership through the development of frameworks and guidance on enterprise risk management, internal control and fraud deterrence.

Who is involved with the Framework update?

PwC serves as the author and project leader for updating the publication, preparing related documents, and reports to the COSO Board of Directors. The PwC Project Team includes senior resources, many whom were involved in previous COSO projects, who bring in-depth understanding of the original *Framework* and the rationale for decisions made in creating that *Updated Document*, as well as additional senior resources that provide current market perspectives.

To capture views of a broad range of professionals in the market place, COSO formed an Advisory Council representing industry practitioners, academia, government agencies, and non-profit organizations.

To what extent are regulators and other oversight bodies involved in this initiative?

The U.S. Federal Deposit Insurance Corporation (FDIC), U.S. Government Accountability Office (GAO), International Federation of Accountants (IFAC), Information Systems Audit & Controls Association (ISACA), and the Risk Management Society (RIMS) have sent observers to attend the Advisory Council meetings and provide input to the project.

Public Exposure

What documents will be exposed for public comment?

Enterprise Risk Management – Aligning Risk with Strategy and Performance, and the Executive Summary are available for public comment.

How long will the public exposure period last?

The COSO Board released the *Enterprise Risk Management – Aligning Risk with Strategy and Performance* for public comments on June 15, 2016 and ended the public exposure period on September 30, 2016.

How can readers provide comments provided during the public exposure?

Any reader wishing to express a point of view on the *Updated Document* released for public comment may do so by providing a comment letter and/or completing the online survey questionnaire at erm.coso.org.

All comment letters received will be available to the public on the COSO website, erm.coso.org, through December 15, 2016.

The COSO Board and the PwC Project Team will carefully consider all the public comment letters and survey responses as they work toward the issuance of the final documents in 2017.

Will comments be confidential?

No, all comment letters will be available to the general public at coso.org, through December 15, 2016.

Additional Information about the Documents

Is adoption of the Framework mandatory?

No, the COSO Board acknowledges that there are many differing regulatory, stakeholder, and industry requirements relating to enterprise risk management. As such, it is incumbent on management to determine if and how to adopt *Enterprise Risk Management – Aligning Risk with Strategy and Performance* to enhance the entity's ability to create, sustain, and realize value.

Has the update been written for a specific regulation or regulatory body?

No, the COSO Board believes there are differing regulatory and stakeholder expectations relating to enterprise risk management and directed the Framework's principles be applicable to all entities regardless of statutes, regulation, and standards.

How does the Updated Framework relate to COSO's 2013 Internal Control–Integrated Framework?

Internal control is positioned within the *Updated Document* as a fundamental aspect of enterprise risk management. Hence the 2013 *Internal Control–Integrated Framework* constitutes an essential building block for enterprise risk management. The two COSO documents complement each other, with neither superseding the other. The updated document will focus on requisite areas that go beyond internal control; however, the *Internal Control–Integrated Framework* remains a viable and suitable framework for designing, implementing, and conducting and assessing the effectiveness of internal control and for reporting, as required in some jurisdictions.

Can I still use the 2004 Enterprise Risk Management–Integrated Framework?

Yes. Since the adoption of the *Updated Document* is not mandatory, management may continue to utilize the 2004 *Framework.* However, COSO reserves the right to supersede or retire the *2004 Enterprise Risk Management–Integrated Framework* in the future.

What entities is *Enterprise Risk Management – Aligning Risk with Strategy and Performance applicable to?*

The *Enterprise Risk Management – Aligning Risk with Strategy and Performance* principles apply to all entities, including not-for-profit and governmental bodies, regardless of size. While some small and mid-size entities may implement the principles of enterprise risk management differently than large entities, they remain applicable to every type of entity.

Who is the intended audience for the Updated Document?

Enterprise Risk Management–Aligning Risk with Strategy and Performance has been drafted for a diverse audience depending on their enterprise risk management roles and responsibilities. The Executive Summary has been drafted for a board level and executive management audience with the intent of summarizing the importance and benefits of enterprise risk management. Specifically, it highlights governance and oversight role of the board as it relates to enterprise risk management. It also provides a synopsis of the components and principles of the Framework.

The Framework is intended to help risk practitioners, business leaders, and assurance providers by offering a comprehensive discussion of the components and principles of the Framework from strategy setting through to execution. These are supported by detailed appendices providing additional examples and insights into the developing and maintaining enterprise risk management practices that are fit for purpose.

Updates to the Document

Why change the title?

The new title - *Enterprise Risk Management—Aligning Risk with Strategy and Performance*, recognizes the importance of the connection between strategy and entity performance with enterprise risk management.

What are the most significant changes from the 2004 Framework?

Please refer to the "Key Changes" section of this FAQ for a more detailed description of some of the most significant changes introduced in *Enterprise Risk Management—Aligning Risk with Strategy and Performance.*

Where is the "COSO cube"?

The "COSO cube" graphic is still being utilized in the COSO *Internal Control – Integrated Framework*. In order to better illustrate the alignment of risk, strategy, and performance *Enterprise Risk Management – Aligning Risk with Strategy and Performance* introduces a new graphic.

Key Changes

The *Updated Document* incorporates significant changes to reflect the evolution of enterprise risk management thinking and practices, and to provide additional clarity on concepts introduced in 2004. Some of the most significant changes are outlined below. Please note that the changes have not been listed in any priority order. The *Updated Document*:

- Adopts a components and principles structure
- Simplifies the definition of enterprise risk management
- Emphasizes the relationship between risk and value
- Renews the focus on the integration of enterprise risk management
- Examines the role of culture
- Elevates discussion of strategy
- Enhances the alignment between performance and enterprise risk management
- Links enterprise risk management into decision-making more explicitly
- Delineates between enterprise risk management and internal controls
- Refines risk appetite and acceptable variation in performance (risk tolerance)

These are each reviewed below.

1. Adopts a structure of components and principles

Similar to other COSO frameworks, the *Updated Document* has been structured using components and principles. The five interrelated Framework components are supported by twenty-three principles that cover topics ranging from risk governance and culture, risk in execution, monitoring risk and performance. Each of the principles represent a fundamental concept associated with a component, are universal in their application, and form part of effective enterprise risk management practices.

The Framework's principal graphic outlines the relationship between the components and principles and serves as a navigational tool throughout the document. The graphic is used to enhance the document's readability, usability, and creates a cohesiveness across the Framework.

2. Simplifies the definition of enterprise risk management

The definition of enterprise risk management in the *Updated Document* was revised to make it more memorable and readable. Feedback from the survey conducted in the *Assess and Envision* phase suggested that while the 2004 version was relatively easy for those in risk management roles to understand, its clarity was less evident to those outside of a risk function. Revising the definition is intended to improve clarity for all users.

The revised version requires that the reader consider the full definition of specific words used in the definition. For instance, the definition of risk ties to the achievement of strategy and objectives, While the definition of enterprise risk management does not directly reference strategy and objectives, it is incorporated through the definition of risk.

Lastly, the updated definition more closely aligns risk to value, which is noted as a key driver of enterprise risk management.

3. Emphasizes the relationship between risk and value

In refining the definition of risk and elevating the discussions of strategy and performance, the *Updated Document* emphasizes the role of enterprise risk management in the creating, preserving and realizing of value. Enterprise risk management is no longer focused principally on preventing the erosion of value and minimizing risk to an acceptable level. Rather, it is viewed as integral to strategy setting and the identification of opportunities to create and maintain value. Instead of simply focusing on reducing risk to a target state, enterprise risk management becomes a dynamic and integral part of the managing an entity throughout the value chain.

4. Renews the focus on the integration of enterprise risk management

The integration of enterprise risk management into all aspects of an organization's operations is highlighted throughout the *Updated Document*. Starting with the integration of enterprise risk management into the strategy-setting process, the setting of business objectives, and managing risk in execution, the consideration of risk is not positioned as an additional or separate activity. Rather, the importance and role of enterprise risk management is presented through the lens of supporting an organization's operations, managing performance and ultimately creating, realizing and preserving value. As an example, the *Updated Document* does not refer to risk reporting but instead on the reporting of potential or actual manifestations of risk impacting performance and the achievement of strategy and business objectives. This *Updated Document* encourages users to consider enterprise risk management as part of the management of an organization as opposed to a distinct or siloed activity.

5. Examines the role of culture

The significance of culture's influence on enterprise risk management practices is one of the first concepts introduced within the *Updated Document*. The importance of understanding and shaping the culture is explored in the context of risk governance and oversight of the entity and how it influences other components of the Framework. For example, the relationship between culture and business context is established at the outset of the Framework. This relationship influences how strategies are chosen and executed. More importantly, it provides the context for the identification and assessment of risks and the allocation of resources in responding to those risks.

6. Elevates discussion of strategy

The *Updated Document* recognizes that some of the most significant organizational failures in recent times have occurred when a strategy is selected that does not align to the mission, vision and core values of an entity. Further, if that that alignment is established, many organizations still do not understand the implications of a selected strategy on their risk profile. Moreover, many organizations are simply caught unaware when seemingly minor failures at an operational level escalate in magnitude and threaten the long term viability of an entity.

The *Updated Document* elevates and expands the discussion of strategy and risk established in 2004 by focusing on the following three concepts:

- The possibility of strategy and business objectives not aligning with mission, vision and values;
- The implications from the strategy chosen; and
- Risk to executing the strategy.

By distinguishing the three potential manifestations of risk impacting strategy, the *Updated Document* provides for a more detailed analysis and recognition of the role and importance of enterprise risk management. The concepts are examined progressively throughout the document, exploring the considerations for the identification, assessment and management of risk and the impact to strategy for each.

7. Enhances the alignment between performance and enterprise risk management

As indicated by its new title, the *Updated Document* enhances the relationship between risk and performance. It focuses on how risk is integral to the establishment of business objectives, and performance targets through the following:

- The *Updated Document* explores how enterprise risk management practices support the identification and assessment of risks that may impact performance.
- By determining the acceptable variations in performance, *Updated Document* users are able to understand how changes in performance may lead to changes in the risk profile of a business objective and vice versa.
- The *Updated Document* emphasizes that risk assessments and risk reporting are not intended to generate long lists of potential risks, but rather highlights how risks may impact the achievement of strategy and business objectives.

To highlight the importance of this relationship, the *Updated Document* introduces a new graphical depiction referred to as a risk profile. The risk profiles demonstrate how the type and severity of risk can change in response to changes in the level of performance for a given strategy or business objective. The depiction also takes into account the entity's risk appetite and helps identify where an organization may be assuming excessive risk or be able to pursue further opportunities. By incorporating the concepts of risk appetite, performance, and risk into a single graphic, the risk profiles offer a dynamic and comprehensive view of risk and enable more risk-aware decision making.

8. Links enterprise risk management into decision-making more explicitly

All organizations recognize that decision-making occurs at every stage of the value chain. As entities seek to create, realize and preserve value, decisions are made around the selection of strategy, the establishment of business objectives and performance targets, and the allocation of resources. Integrating enterprise risk management into the lifecycle of an entity supports risk-aware decision-making.

The *Updated Document* progressively explores how information gathered about the organization's risk profile enhances overall decision-making. This information includes the understanding of the severity and type of risk, the influence of the business context, the understanding of assumptions underpinning the identification and assessment of risk, and the entity's risk culture and appetite.

9. Delineates between enterprise risk management and internal controls

The *Updated Document* neither replaces, nor supersedes, the *2013 Internal Control – Integrated Framework*. The two frameworks are distinct but complementary. Those familiar with *Internal Controls – Integrated Framework* will note that both frameworks use a structure of components and principles, however these are tailored to each.

To avoid redundancy, some aspects of internal control common to both are not repeated in the *Updated Document*. Perhaps the most prominent of these is control activities. However some aspects introduced in *Internal Control–Integrated Framework* such as governance aspects of enterprise risk management are further developed in this enterprise risk management document.

10. Refines risk appetite and acceptable variation in performance (risk tolerance)

The *Updated Document* refines the concepts of risk appetite and acceptable variation in performance (often referred to as risk tolerance). Risk appetite continues to be defined as the amount of risk an entity is willing to accept in the pursuit of its strategy and business objectives. Risk tolerance is however, now articulated using the language of performance and not representative of a more granular or detailed version of risk appetite. In the risk profiles, this relationship is represented by the perpendicular intersection of the risk appetite and performance lines.

By refining the definition of risk tolerance, the focus is now on determining the amount of risk that is acceptable for a given level of performance. Organizations are able to articulate the boundaries of acceptable risk in the context of performance. The determination of those boundaries enables organization to better assess whether changing levels of performance remain within the limits of acceptable variation. No longer are either risk or performance considered static and separate, but rather constantly changing and influencing one another.