COSO ERM Framework and the Federal Government

Integrating Risk with Strategy and Performance

The risk landscape has evolved, the complexity of risk has changed, new risks have emerged, and both senior leaders and executives have enhanced their awareness and oversight of Enterprise Risk Management (ERM) while asking for improved risk reporting. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) recommissioned Guidehouse to lead the update to the 2004 ERM Framework now titled *Enterprise Risk Management—Integrating with Strategy and Performance* to respond to these dramatically changing circumstances and provide guidance to the global ERM community.

The 2016 Federal Enterprise Risk Management Survey conducted by Guidehouse and the Association for Federal Enterprise Risk Management (AFERM) showed the COSO ERM Framework as the most widely adopted framework among respondents, with 46% indicating they predominantly follow the COSO ERM Framework and an additional 23% indicating they follow the COSO ERM Framework in combination with ISO 31000.

69% of Federal ERM Programs follow the COSO Framework predominantly or in conjunction with ISO 31000, according to the 2016 AFERM/Guidehouse ERM Survey, making it the most widely adopted framework among respondents.

Federal agencies need to understand how ERM is evolving, as shown in the new Framework, and understand the implications. This paper provides a summary of some of the key things that are new in the updated Framework and some thoughts on what this means for Federal agencies.

Highlights of the New Framework

In a constantly evolving political, social, and business climate, Federal agencies and organizations must 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. In addition, stakeholders are seeking greater transparency and accountability, which means organizations need defensible and consistent decision-making throughout the organization.

Enterprise Risk Management—Integrating with Strategy and Performance focuses on integrating risk management with strategy setting and the day-to-day management and decision-making of implementing strategy. The publication also focuses on management of risk across the business and at all altitudes of the organization. It also recognizes the importance of culture in support of how the organization considers risk.

COSO ERM Definition

The culture, capabilities and practices, integrated with strategy setting and its execution, that organizations rely on to manage risk in creating, preserving and realizing value

For more information, please contact:

David Fisher
Managing Director
(703) 610-7505
dfisher@guidehouse.com

Kate Sylvis
Director
(571) 246-1985
ksylvis @guidehouse.com

Integration of risk, strategy and performance

The Framework elevates the discussion of integrating strategy and risk through three different dimensions:

1. The possibility of strategy not aligning with mission, vision and core values
2. The implications from the strategy chosen
3. Risk to strategy and performance

The most significant causes of value destruction are embedded in the possibility of the strategy not supporting the agency's mission and vision, and the implications from the strategy chosen.

ERM enhances strategy selection. Choosing a strategy calls for structured decision-making that analyzes risk and aligns resources with the mission. By deploying ERM capabilities as part of selecting and refining a strategy, management will gain a better understanding of how the explicit consideration of risk may impact the choice of strategy.

ERM also strengthens the connection of strategy and risk to performance. Performance objectives are developed and considered through the risk lens allowing agencies to improve their ability to identify risks and establish appropriate responses, reducing surprises and related costs or losses, while pursuing advantages.

Rather than being considered and managed in a silo, the full spectrum of the organization's risks can be understood as an interrelated strategically-aligned portfolio of organizational challenges and opportunities to be effectively managed as it pursues work to ensure a successful mission.

Decision making and resilience

ERM can also enhance enterprise resilience—the ability to anticipate and respond to change, determine how it could impact performance, and create needed shifts in strategy. With regular monitoring of changes in the political and operational environment (business context) and the effect these changes may have on risk and performance, an organization is better prepared to predict and respond to fluctuations in performance.

Governance and culture

The Framework's principles on culture are now more focused on aligning the core values and risk appetite of the organization to promote consistent and risk-based decision making. It deepens the development of meaningful risk information in support of strong governance that effectively integrates risk with strategy and performance to effectively manage the business and achieve better outcomes.

Multiple altitudes of risks

The importance of recognizing the risks that emanate and must be managed at all levels of the organization solidifies ERM as more than just an isolated view of risk in the business. The Framework explores how risks can manifest at multiple levels within an organization with some risks directly impacting the entity's strategy while others impacting business objectives. The Framework also addresses how risks can change in severity and prioritization at different levels of the organization and how the impacts of correlation and diversification are considered when analyzing the portfolio view of risk.

Case study: Integration of Risk, Strategy and Performance in the Federal Government

Guidehouse supported the development and implementation of an innovative Enterprise Risk Management program at a Federal agency that exemplifies the updates in the new COSO Framework. This Agency's ERM Program purposefully aligns strategy setting, performance management, risk management, and internal controls. Guidehouse supported this Agency's annual strategy setting development using risk and changes in business context as an input to develop strategic outcomes that align with the Agency's mission. An executive council monitors enterprise-level risks and risks against performance outcomes in pursuit of strategic goals. Senior leadership uses this information to determine risk responses and inform resource allocation.

The image to the right illustrates the Agency's alignment of ERM with strategy setting, risk management, performance management, and internal control activities. This construct provides clear linkages between these interrelated activities and enables targeted reporting and communications to support risk-based decision making at multiple altitudes of the Agency.