protiviti®
Risk & Business Consulting.
Internal Audit.

Volume 6, Issue 2

The Bulletin

Updated COSO ERM Framework: What's New?

On June 14, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) released its *Enterprise Risk Management – Aligning Risk with Strategy and Performance* for public exposure and comment during a period to expire September 30, 2016.[1] Those familiar with the 2004 Enterprise Risk Management – Integrated Framework, which the new framework updates, will likely not consider the concepts included in the updated framework as being completely "new." However, they will notice the emphasis is markedly different: It's about focusing on what is really important in making enterprise risk management (ERM) work within an organisation.

Why Update? The Past 10 Years Revisited

Following the original framework's publication in 2004, companies implementing it encountered some issues, the most formidable being the distraction of all-hands-on-deck efforts by companies listing their stock on U.S. stock exchanges to comply with Sarbanes-Oxley Act legislation.

There were other implementation challenges, as well:

- Attempts to implement ERM were often not enterprisewide in scope, and applications of ERM were rarely integrated with strategy-setting. Thus, the most important and distinctive aspects of COSO's definition of ERM in the framework – "applied in strategy-setting and across the enterprise" – were either misunderstood or ignored in practice.
- In the developmental process, COSO built the framework off of the familiar cube underlying the internal control framework. Despite COSO modifying the right side of the cube to delete references to activities and processes and incorporate a broader focus on the entity and its operating units and divisions, many organisations attempted to implement the framework at too granular a level, as if to apply it at the process level rather than in strategy-setting. The ERM implementation initiative therefore suffered from becoming mired in minutiae, and many C-level executives quickly lost interest.
- Some organisations tried to implement ERM as an assurance initiative, rather than as a way to run and manage the business better. This approach proved to be a nonstarter in many organisations when dealing with leaders of operating units, particularly when the initiative positioned internal audit as the lead.
- The Great Recession set in motion by the financial crisis of 2008 initially triggered another distraction as many companies were forced into crisis mode.
- In the end, it took dramatic events with a long reach – the financial crisis of 2008 and, to a lesser extent, the Japanese tsunami in 2011 – to trigger real interest in ERM.

Simply stated, the attention span of executives was limited when COSO issued its framework, and implementation in practice has been uneven ever since.

For all of these reasons, the ERM framework didn't really get a fair shot in its early years. Until the financial crisis, many senior executives were either unaware of the framework or unsure what to do with it. However, once the financial crisis occurred, the issues and value proposition became clearer.

An entire industry virtually ran the proverbial bus off the cliff, triggering a brutal global recession. The crisis taught valuable lessons regarding the potential for the unexpected, with such terms as "black swan" entering the business lexicon. The lessons demonstrated the vital importance of several key elements of effective risk management – a fully engaged board, a bought-in chief executive officer (CEO), an open and transparent culture, a compensation structure that balances the short and long term and, most important, the will and discipline of management to act in a contrarian manner when the warning signs indicate danger is at hand. These elements require constant vigilance to preserve and sustain ERM.

Thus, the value of being an early mover ahead of the herd became easier to recognise. Boards began asking different and tougher questions. CEOs started looking for ways to focus their dialogue with the board and get the attention of their organisations regarding risk-related matters.

[1] *Enterprise Risk Management – Aligning Risk with Strategy and Performance*, COSO, June 2016 Exposure Draft, available at www.coso.org.

One other development worth noting is the continued dramatic change in the business environment as it has become clear that the half-life of business models is compressing. Powerful megatrends have emerged that can potentially disrupt established business models more quickly than ever, not the least of which are the steady advances in digital technologies, resulting in unprecedented amounts of information being consumed and generated by consumers and businesses. We've also seen the Arab Spring, increasing national sentiment and geopolitical tensions, aging populations, rising cyber-dependency, increasing income disparity, the emergence of a terrorist caliphate, massive migration flows and, more recently, the collapse of oil prices – to name just a few developments.

THE UNEVEN IMPLEMENTATION OF THE 2004 FRAMEWORK, DRAMATIC RISK MANAGEMENT BREAKDOWNS SINCE 2004 AND THE INCREASING COMPLEXITY OF THE BUSINESS ENVIRONMENT HAVE COMBINED TO CREATE A CRY FOR CLARITY.

The reality is clear: To stay ahead of the disruption curve, business leaders must quickly discern the vital signs of change and the related implications to their markets and business models.

In summary, the uneven implementation of the 2004 framework, dramatic risk management breakdowns since 2004 and the increasing complexity of the business environment have combined to create a cry for clarity. Amid this cry, COSO saw an opportunity to connect ERM more clearly with a multitude of stakeholder expectations; position risk in the context of an enterprise's performance, rather than as the focus of an isolated exercise; and enable organisations to become more anticipatory. Indeed, institutions positioned as early movers see changes on the horizon as potential market opportunities rather than solely as potential crises.

What's New? A Principles-Based Approach

COSO's updated framework begins with an underlying premise that every entity exists to provide value for its stakeholders and faces uncertainty in the pursuit of that value. The term "uncertainty" is defined as something not known. "Risk" is considered to be the effect of such uncertainty on the formulation and execution of the business strategy and the achievement of business objectives. Therefore, according to the updated framework:

[O]ne challenge for management is to determine how much uncertainty – and therefore how much risk – the organisation is prepared and able to accept. Effective [ERM] allows management to balance exposure against opportunity, with the goal of enhancing capabilities to create, preserve and ultimately realise value.

This emphasis on the relationship between risk and value underlies COSO's attempt to simplify and focus its definition of ERM:

The culture, capabilities and practices integrated with strategy-setting and its execution, that organisations rely on to manage risk in creating, preserving and realising value.

The title of the updated framework recognises the increasing importance of the connection among risk, strategy and enterprise performance. According to COSO, the new framework:

- Provides greater insight into strategy and the role of ERM in setting and executing strategy;
- Enhances alignment between organisational performance and ERM;
- Accommodates expectations for governance and oversight;
- Recognises the continued globalisation of markets and operations and the need to apply a common, albeit tailored, approach across geographies;
- Presents fresh ways to view risk in the context of greater business complexity;
- Expands risk reporting to address expectations for greater stakeholder transparency; and
- Accommodates evolving technologies and the growth of data analytics in supporting decision-making.

In the updated framework, COSO introduces five interrelated components and, similar to how the internal control framework was updated in 2013, outlines relevant principles for each component. The components and principles are discussed below.

BOTH RISK GOVERNANCE AND RISK CULTURE ARE NEEDED TO LAY A STRONG FOUNDATION FOR EFFECTIVE ERM.

Importance of Risk Governance and Culture

The first component of the updated framework forms a basis for the other four components of ERM. Risk governance sets the institution's tone and reinforces the importance of and establishes oversight responsibilities for ERM. Culture pertains to ethical values, responsible business behaviour, and understanding of the business context, and is reflected in decision-making. Both risk governance and risk culture are needed to lay a strong foundation for effective ERM. There are six principles underlying this foundational component.

Risk Governance and Culture

1. Exercises Board Risk Oversight
2. Establishes Governance and Operating Model
3. Defines Desired Organisational Behaviours
4. Demonstrates Commitment to Integrity and Ethics
5. Enforces Accountability
6. Attracts, Develops and Retains Talented Individuals

Exercises Board Risk Oversight – Risk governance and culture start at the top of the organisation with the influence and oversight of the board of directors. Board members must be accountable and responsible for risk oversight and possess the requisite skills, experience and business knowledge to provide that oversight. When the board is composed of an independent majority, it serves as an effective check and balance on executive management and institutional bias.

COSO asserts that "risks to the strategy" is not the only dimension of risk to consider strategically. There are two additional dimensions to consider in strategy-setting that can significantly affect an enterprise's risk profile.

Establishes Governance and Operating Model – An enterprise's strategy is executed by management's organisation and execution of day-to-day operations to achieve business objectives. As the operating model typically reflects the legal and management structure with the accompanying reporting lines, how it is administered and governed can introduce new and different risks or complexities that may affect the enterprise's strategic execution, management of risk and achievement of objectives. Therefore, the ERM process must take into account the risk profile associated with the enterprise's operating model.

Defines Desired Organisational Behaviours – COSO frames desired behaviours within the context of the enterprise's core values and attitudes toward risk. Whether an institution considers itself to be risk averse, risk neutral or risk aggressive, COSO suggests that it encourage a risk-aware culture. Such a culture is characterised by strong leadership, a participative management style, accountability for actions as well as results, an explicit embedding of risk in decision-making processes, and open and positive risk dialogues. These characteristics integrate risk into the day-to-day business.

Demonstrates Commitment to Integrity and Ethics – It is noteworthy that COSO focuses on the tone throughout the organisation. While tone at the top is defined by the operating style and personal conduct of management and the board of directors, it must be driven deep down into the entity. This means the tone in the middle must be aligned with the tone at the top so that the tone at the bottom reflects the desired core values and risk attitudes.

Tone across the organisation is boundaryless, meaning both the entity's personnel and its business partners must be responsive to the expectations set by management and the board. Therefore, standards of conduct must be established and evaluated, and any deviations from those standards must be addressed in a timely manner. Open communication and transparency about risk and risk-taking expectations are vital to setting the appropriate tone.

Enforces Accountability – Individuals at all levels of the entity must be accountable for ERM. Just as important, the institution must hold *itself* accountable for providing the appropriate standards and guidance regarding ERM. This accountability starts at the top with the board and the CEO, and is driven down into the enterprise through the appropriate performance expectations, incentives and reward systems. The board and CEO must be vigilant in ensuring that pressures within the institution do not drive irresponsible and/or illegal behaviour.

To this point, COSO states that excessive pressures that can lead to such behaviour are most commonly associated with unrealistic performance targets, conflicting business objectives of different stakeholders, and an imbalance between rewards for short-term financial performance and expectations of stakeholders focused on the long term (corporate sustainability targets). COSO also asserts that pressures can be created both internally (through inappropriate performance incentives or changes in strategy) and externally (such as shifts in customer needs having an impact on sales performance or a disruptive change affecting the viability of the operating model).

Attracts, Develops and Retains Talented Individuals – Finally, risk governance and culture recognise the importance of building the human capital and talent of individuals in alignment with business objectives. Management must define the knowledge, skills and experience needed to execute the strategy; set appropriate performance expectations; attract, develop and retain the appropriate personnel and strategic partners; and arrange for succession.

A Multidimensional Focus in Strategy-Setting

Many institutions focus on identifying risks to the execution of the strategy. However, in this second ERM component, COSO asserts that "risks to the strategy" is not the only dimension of risk to consider strategically. There are two additional dimensions to consider in strategy-setting that can significantly affect an enterprise's risk profile. The second dimension is the "possibility of strategy not aligning" with the enterprise's mission, vision and core values that define what it is trying to achieve and how it intends to conduct business. A misaligned strategy increases the possibility that, even if successfully executed, the enterprise may not realise its mission and vision.

The third dimension to consider is the "implications of the strategy chosen." COSO states:

When management develops a strategy and works through alternatives with the board, they make decisions on the tradeoffs 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 within the organisation's risk appetite, and how it will help drive the organisation to set objectives and ultimately allocate resources efficiently.

In summary, the updated COSO framework elevates the discussion of strategy and the integration of ERM with strategy by asserting that all three dimensions need to be considered as part of the strategy-setting process. There are five principles underlying the risk strategy and objective-setting component of ERM.

Risk Strategy and Objective-Setting

7. Considers Risk and Business Context
8. Defines Risk Appetite
9. Evaluates Alternative Strategies
10. Considers Risk When Establishing Business Objectives
11. Defines Acceptable Variation in Performance

Considers Risk and Business Context – The updated framework views the business context through the lens of the external and internal environments. It also considers the role of internal and external stakeholders whose influence can significantly shape the external and internal environments. The point is that management must consider risk from changes in the business context and adapt accordingly in executing strategy and achieving business objectives.

Defines Risk Appetite – The organisation defines risk appetite in the context of creating, preserving and realising value. The risk appetite statement is considered during the strategy-setting process, communicated by management, embraced by the board and integrated across the entity. Risk appetite is shaped by the enterprise's mission, vision and core values and considers its risk profile, risk capacity, risk capability and maturity, culture, and business context.

Evaluates Alternative Strategies – Alternative strategies are built on different assumptions – and those assumptions may be sensitive to change in different ways. The organisation evaluates strategic options and sets its strategy to enhance enterprise value, considering risk resulting from the strategy chosen. Change in key factors can invalidate the assumptions underlying the strategy. Boards and executive management should understand these sensitivities – the implications of the strategy – before they approve a strategy. If the strategy is approved, the factors in the environment that could invalidate the critical assumptions must be identified and monitored over time.

Considers Risk When Establishing Business Objectives – Management establishes objectives that align with and support the strategy at various levels of the business. These objectives should consider, and be aligned with, the entity's risk appetite. In effect, an organisation's business objectives must cascade downward through its various divisions, operating units and functions.

Defines Acceptable Variation in Performance – COSO defines the "acceptable variation in performance" (sometimes referred to as risk tolerance) as the range of acceptable outcomes related to achieving a specific business objective. While risk appetite is broad, acceptable variation in performance is tactical and operational. Acceptable variation in performance relates risk appetite to specific business objectives and provides measures that can identify when risks to the achievement of those objectives emerge. It is often measured using the same methodology employed to measure achievement of business objectives, whether those objectives pertain to customer fulfillment, cost performance, elapsed time, process and product innovation, or employee engagement. Operating within acceptable variation in performance provides management with greater confidence that the entity remains within its risk appetite; in turn, this provides a higher degree of comfort that the organisation will achieve its business objectives in a manner consistent with its mission, vision and core values.

Getting a Grip on Risk

Risks that could impact the achievement of strategy and business objectives need to be identified and assessed. These "risks in execution" must be prioritised in terms of severity and in the context of risk appetite. The organisation then selects risk responses and takes a portfolio view of the amount of risk it has undertaken. This third ERM component is supported by six principles.

Risk in Execution

12. Identifies Risk in Execution
13. Assesses Severity of Risk
14. Prioritises Risk
15. Identifies and Selects Risk Responses
16. Assesses Risk in Execution
17. Develops a Portfolio View

Identifies Risk in Execution – The institution identifies new and emerging risks, as well as changes to known risks to the execution of its strategy, to achieve its business objectives. The risk identification process should consider risks arising from a change in business context and risks currently existing but not yet known.

Assesses Severity of Risk – Depending on the anticipated severity of the risk, COSO suggests the use of qualitative and quantitative approaches in assessment processes.

Qualitative assessment approaches may be used when risks do not lend themselves to quantification or when it is neither practicable nor cost-effective to gather sufficient data to enable quantification. As COSO noted, management may use scenario analysis in assessing risks that could have an extreme impact, and may find simulations more useful when assessing the effects of multiple events. Conversely, high-frequency and low-impact risks may be more suited to data analysis or other internal information, as well as workshops and interviews, to determine the severity of the risk. For risks that are more easily quantifiable, or where greater granularity or precision is required, a probability modelling approach may be appropriate.

Prioritises Risk – The organisation prioritises risks as a basis for selecting risk responses using appropriate criteria. Risk criteria might include adaptability, complexity, velocity, persistence and recovery. In addition, risks that approach the boundaries of acceptable variation in performance of the entity's established business objectives or risk appetite are typically given higher priority.

Identifies and Selects Risk Responses – For identified risks, management selects and deploys an appropriate risk response. Risk responses may accept, avoid, exploit, reduce and share risk. In selecting risk responses, management considers such factors as the business context, costs and benefits, obligations and expectations, the prioritisation and severity of the risk, and the enterprise's appetite for risk.

Assesses Risk in Execution – Once a risk response is selected and implemented, it must be evaluated to ensure it is performing as intended. The task of assessing risk responses is typically owned by those accountable for the effective management of identified risks and by assurance providers who seek insight into the entity's performance and effectiveness of its risk responses. In discharging their governance and oversight responsibilities, management and the board of directors are informed by the transparency gained through the assessment of responses to critical enterprise risks.

Develops a Portfolio View – ERM requires the institution to consider risk from an entity-wide, or portfolio, perspective. COSO states that a "portfolio view" is a composite view of risk the organisation faces relative to its business objectives, which allows management and the board to consider the nature, likelihood, relative size and interdependencies of risks, and how they may affect performance. Through a portfolio view, the institution identifies risks that are significant at the enterprise level and determines whether the entity's residual risk profile aligns with its overall risk appetite.

Maximising the Value of Risk Information and Reports

The fourth ERM component recognises the vital need for a continuous process to obtain and share relevant information from internal and external sources; this information for decision-making must flow up, down and across the organisation. The process provides the necessary insights to key risk stakeholders. Four principles support this component.

Risk Information, Communication and Reporting

18. Uses Relevant Information
19. Leverages Information Systems
20. Communicates Risk Information
21. Reports on Risk, Culture and Performance

Uses Relevant Information – COSO defines "relevant information" as information that facilitates making informed business decisions. The more information contributes to increased agility, greater proactivity and better anticipation, the more relevant it is and the more likely the organisation will execute its strategy successfully, achieve its business objectives, and establish sustainable competitive advantage.

Leverages Information Systems – Information systems that consist of people, data and technologies provide the institution with the data and information it needs to support ERM. COSO asserts there is no one-size-fits-all system; however, the choice of technology and/or tools supporting an entity's information system and the design of that system can be critical to executing the strategy and achieving business objectives. Factors influencing technology selection and implementation include the entity's goals, marketplace needs, competitive requirements, and the associated costs and benefits.

Communicates Risk Information – The institution reports on risk at multiple levels of and across the enterprise. Organisations use different channels to communicate risk data and information to internal and external stakeholders. These channels enable management, with oversight from the board, to make more informed decisions to advance the strategy and achieve established business objectives.

Reports on Risk, Culture and Performance – Risk reporting encompasses the information required to support or enhance decision-making and to enable the board of directors and others to fulfill their risk oversight responsibilities. There are many different types of reports on risk, culture and performance. These reports combine quantitative and qualitative risk information with varying presentations, ranging from fairly simple to more complex, depending on the size, scope, scale and complexity of the organisation.

Risk information may focus on a particular area or segment within the business or on a particular type of risk or group of related risks. Risk reporting is tailored to different levels within the organisation and supports the enterprise's decision-making processes; however, management must exercise judgement when using reported data and information and making key decisions.

Monitoring What Really Matters

The fifth and last component focuses on how the organisation monitors risk management performance and how well the components of ERM function over time in view of substantial changes. Effective monitoring processes enable the institution's leaders to gain insight into the relationship between risk and performance, understand how risks from the strategy are affecting performance, and identify emerging risks in achieving the strategy. This component is supported by two principles.

Monitoring Risk Management Performance

22. Monitors Substantial Change
23. Monitors ERM

Monitors Substantial Change – If not considered on a timely basis, change can create significant performance gaps vis-à-vis competitors or invalidate the critical assumptions underlying the strategy. Monitoring of substantial change is built into business processes in the ordinary course of running the business and conducted on a real-time basis.

Monitors ERM – ERM is like any other process. It should be improved continuously over time. Even those entities with a mature ERM process can become more efficient and effective in increasing its value contributed. As ERM is integrated across the entity, embedding continuous evaluations can systematically identify improvements. Separate evaluations (by internal audit, for example) also provide an occasion to identify opportunities to improve ERM.

Implications for Boards and Executive Management

COSO's updated ERM framework provides ample food for thought for organisational leaders to consider. The principles-based approach embodied by the framework recognises that there is no one-size-fits-all solution. Every organisation is distinguished from others by its industry, strategy, structure, culture, business model and financial wherewithal.

From a practical standpoint, companies can implement the framework in a manner that makes the most sense in light of their facts and circumstances. We believe it is a worthwhile exercise for an enterprise's leaders to use the updated framework to evaluate their approach to managing risk with the objective of strengthening it to enable them to face the future with confidence. Some issues may be controversial, such as fully integrating risk with strategy-setting. But ignoring those issues may prove costly – or even lethal – for a business operating in today's unpredictable world.

Summary

In updating its ERM framework, COSO asserts that organisations need to become more adaptive to change, and management needs to adopt better thinking on how to manage the increasing volatility, complexity and uncertainty in the marketplace. COSO has targeted its updated framework to meet the needs of boards and executive management with a principles-based approach that integrates risk with strategy and performance. Interested parties have an opportunity to offer their points of view and feedback to COSO on the updated framework by providing a comment letter and/or completing an online survey questionnaire at erm.coso.org. COSO expects to issue the final framework around the end of 2016.

Let's Talk

"We believe it is a worthwhile exercise for an enterprise's leaders to use the updated framework to evaluate their approach to managing risk with the objective of strengthening it to enable them to face the future with confidence."

Join the COSO ERM conversation at

www.protiviti.com/cosoerm.

protiviti®
Risk & Business Consulting.
Internal Audit.

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.
© 2016 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. PRO-0816