ISSUE 95

protiviti®
Face the Future with Confidence

Board Perspectives:
Risk Oversight

Time to Take a Fresh Look at ERM

Now that the Committee of Sponsoring Organizations of the Treadway Commission (COSO) has released its updated framework on enterprise risk management (ERM),[1] it's time for companies to take another look at their risk management practises. In this issue, we summarise our views on how organisations should approach this process.

While the concepts in the update aren't new, the emphasis is markedly different, with a focus on what's really important in maximising the value of ERM. Since the 2007–2008 financial crisis, many ERM implementations have been oriented around answering three questions:

1. Do we know what our key risks are?
2. Do we know how they're being managed?
3. How do we know?

In responding to these three questions, executive management and boards in some companies have made progress in differentiating the truly critical enterprise risks from the risks associated with day-to-day business operations.

While seeking these answers is a useful exercise, is it enough? To make that determination, organisations should also consider the following questions:

- **Will our ERM approach help us to identify a strategic error in time?** Based on a study of more than 1,000 large U.S. public companies,[2] 81 percent of those businesses experiencing dramatic losses of enterprise value over a 10-year period incurred those losses due to major strategic blunders. The study was based on the premise that all of the occurrences contributing to the losses should have been anticipated. Obviously, they weren't. The bottom line: If organisations focus ERM more on operational, financial and compliance issues than on strategic issues, they risk overlooking strategic errors. The speed of risk and change demands a sharper focus on strategic risk.

[1] *Enterprise Risk Management — Integrating with Strategy and Performance*, COSO, Sept. 2017, available at www.coso.org/Pages/erm.aspx.

[2] "The Lesson of Lost Value," Christopher Dann, Matthew Le Merle and Christopher Pencavel, *Strategy+Business*, Nov. 27, 2012: www.strategy-business.com/article/00146?gko=f2c51. Note: This study is the most recent one we could find. As it is based on the period ending Dec. 31, 2011, we recognise that a more recent study period might reflect different results. For example, a study period since 2008 would reduce the effect of failures resulting from the 2007-2008 financial crisis and incorporate the more recent trend of digital transformation. Since the crisis, the capital markets have increased; therefore, it's likely that many of the "losers" of enterprise value are companies that deployed flawed strategies and/or failed to adapt to shifting markets. Whatever the actual percentage, we believe it to be significant.

- **Is our organisation able to recognise the signs of disruptive change, and is it agile and resilient enough to adapt to change?** Powerful megatrends in the digital economy can potentially disrupt established businesses and continue to compress business model half-lives. To stay ahead of the disruption curve, business leaders must quickly discern the vital signs of change and how they affect their markets and business models. What good is ERM if it isn't helping organisations position themselves as early movers in these dynamic times?

- **Will our CEO "dance until the music stops"?** Just before the 2007-2008 financial crisis, when the CEO of a major global bank was asked about the risks his bank was taking in the U.S. subprime mortgage market, he made the famous comment that "as long as the music is playing … we're still dancing."[3] That quote is the stuff of legends, as it raises the question as to whether an organisation truly considers risk and return in its decision-making or just blindly follows the herd. More important, it illustrates the difficulty of exiting a market that is generating significant revenue and profits — despite excessive risk. Emotional investment in the existing business model and an unshakable bias in favour of sustaining that model can be dangerous.

- **Do we seek out what we don't know? Are we prepared for the unexpected?** "Stuff happens" is *the* lesson from the financial crisis. It was learned again in the Japanese tsunami in 2011. No organisation or brand is immune to the risk of surprise. Is ERM facilitating organisational preparedness for a high-impact, high-velocity and high-persistence risk event?

- **Is everyone competing for capital and funding with rose-coloured glasses?** Is management reducing the risk of bias in decision-making processes involving resource and budget allocations? Are both risk and opportunity considered when significant investments and capital expenditures are proposed to ensure that resources are allocated to their highest and best use? Resource and budget allocations needn't be a grabfest.

Yes, companies have made progress, but depending on the answers to the above questions, more needs to be done.

COSO's Framework Could Alter the Conversation

The updated framework clarifies the importance of the connection between risk, strategy and enterprise performance. Its title says it all: "Integrating with Strategy and Performance." It begins with an underlying premise that every entity exists to provide value for its stakeholders and faces uncertainty in the pursuit of that value. Therefore, the framework itself focuses on preserving and creating enterprise value with an emphasis on managing risk within the entity's risk oversight. The framework states:

> [T]he challenge for management is to determine how much uncertainty — and therefore how much risk — the entity is prepared and able to accept. Effective [ERM] allows management to balance risk and opportunity, with the goal of enhancing the capacity to create, preserve, and ultimately realise value.

The framework introduces five interrelated components and outlines 20 relevant principles arrayed among those components. Its principles-based structure is a significant improvement over its 2004 counterpart, as it offers a benchmarking option for companies seeking to enhance their ERM approach. The framework focuses on integrating ERM with the core processes that matter, a concept that is embodied in the definition of ERM: "The culture, capabilities and practises integrated with strategy-setting and performance, that organisations rely on to manage risk in creating, preserving and realising value." While a stand-alone process may be worthwhile and useful, it is not ERM as COSO defines it.

The following observations address critical aspects of ERM, as envisioned by COSO:

- **Integrate ERM with strategy.** COSO asserts that there are three dimensions to integrating ERM with strategy-setting and execution: risks to the execution of the strategy; implications from the strategy (meaning each strategic option has its unique risk-reward trade-off and risk profile); and the possibility of the strategy not aligning with the enterprise's mission, vision and core values. All three dimensions need to be considered as part of the strategic management process.

[3] "Citigroup's Chuck Prince Wants to Keep Dancing, and Can You Really Blame Him?", *Time* magazine, July 10, 2007: http:// business.time.com/2007/07/10/citigroups_chuck_prince_wants/.

- **Integrate risk with performance.** COSO makes it clear that risk reporting is not an isolated exercise or appendage. Operating within the bounds of an acceptable variation in performance provides management with greater confidence that the entity will achieve its business objectives and remain within its risk appetite.
- **Lay the foundation for ERM with strong risk governance and culture.** The board and CEO must be vigilant in ensuring that pressures within the organisation are neither excessive nor incenting unintended consequences (e.g., unmanageable bias, flawed decisions, and irresponsible and/or illegal behaviour). Such pressures may be spawned by unrealistic performance targets, conflicting business objectives of different stakeholders, disruptive change altering the fundamentals underlying the business model, and imbalances between rewards for short-term financial performance and stakeholders focused on the long term.
- **Tie risk considerations into decision-making processes.** COSO defines "relevant information" as information that facilitates informed decision-making. The more information contributes to increased agility, greater proactivity and better anticipation of changes to the enterprise, 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.

Every organisation is different according to its industry, strategy, structure, culture, business model and financial wherewithal. As companies use the COSO framework to evaluate their current ERM approach, boards should urge senior executives to address the above elements of ERM.

Three Keys to Advancing ERM

In advancing ERM within the organisation, we suggest organisations focus on three keys:

Key #1: Position the organisation as an early mover. When a market shift creates an opportunity to create enterprise value or invalidates critical assumptions underlying the strategy, it may be in an organisation's best interests to recognise that insight and act on it as quickly as possible. The following questions apply to every organisation: When the entity's fundamentals change, which side of the change curve will it be on? Will it be facing a market exploitation opportunity, or will it be looking at the emerging risk of an outdated strategy? The organisation attains time advantage when it obtains knowledge of a unique market opportunity or an emerging risk and creates decision-making options for its leaders before that knowledge becomes widely known.

Key #2: Address the challenges of risk reporting. Consistent with the objective of being an early mover, risk reporting should help organisations become more agile and nimble in responding to a changing business environment. To truly impact decision-making, risk reporting must address three questions:

- Are we riskier today than yesterday?
- Are we entering a riskier time?
- What are the underlying causes?

Risk reporting is often not actionable enough to support decision-making processes. Until it is designed to answer these three questions, it won't be. And once it is, it becomes the key to evolving ERM from a "risk listing" process to a "risk-informed" decision-making discipline.

Key #3: Preserve reputation by maximising the lines of defence. How do organisations safeguard themselves against reputation-damaging breakdowns in risk and compliance management? The widely accepted lines-of-defence model consists of three lines of defence. The first line consists of the business unit management and process owners whose activities give rise to risk. The second line consists of the independent risk and compliance functions, and internal audit is the third line. The tone of the organisation represents the collective impact of the tone from the top, the tone from the middle and the tone at the bottom on risk management, compliance and responsible business behaviour. The proper tone lays the cultural foundation for the effective functioning of each of the three lines of defence. Arguably, the final line of defence is senior management and the board. For example, top management acts on risk information on a timely basis when significant issues are escalated and involves the board when necessary.

These three keys offer a focused line of sight for companies seeking to advance their ERM approach consistent with the updated COSO framework.

Forget about ERM being an overlay on the core business processes that matter. If senior managers are concerned about that, their advisers either don't understand what ERM is — given how COSO has defined it — or are asking the wrong questions. Companies have a choice in driving the maturity of their ERM approach as there is no one-size-fits-all solution regarding how to implement it. However, the elements summarised above must be addressed effectively.

The relationship of ERM to the processes the CEO values can be compared to the contribution of salt, pepper and other seasonings to a sumptuous meal. The whole idea is to enhance the odds of the organisation achieving its objectives by enabling it to become more adaptive in an increasingly volatile, complex and uncertain world.

Questions for Boards

Following are some suggested questions that boards of directors may consider, based on the risks inherent in the entity's operations:

- Is the board satisfied that the organisation is adaptive to change, and is management considering the effects of volatility, complexity and uncertainty in the marketplace when evaluating alternative strategies and executing the strategy?
- Should management consider the principles that are supporting effective implementation of ERM, as set forth by COSO, to ascertain whether improvements are needed to the enterprise's risk management approach?

How Protiviti Can Help

Protiviti assists boards and executive management with assessing the enterprise's risks, either across the entity or at various operating units, and the capabilities for managing those risks. The firm works closely with companies to ascertain the most effective ways to integrate risk within their core management processes. The firm assists with both assessing and improving the entity's ERM approach, as well as implementing strategies, tactics and success measures for managing and reporting specific strategic, financial, operational, technology and other risks.

Is It Time for Your Board to Evaluate Its Risk Oversight Process?

The TBI Protiviti Board Risk Oversight Meter™ provides boards with an opportunity to refresh their risk oversight process to ensure it's focused sharply on the opportunities and risks that truly matter. Protiviti's commitment to facilitating continuous process improvement to enable companies to confidently face the future is why we collaborated with The Board Institute, Inc. (TBI) to offer the director community a flexible, cost-effective tool that assists boards in their periodic self-evaluation of the board's risk oversight and mirrors the way many directors prefer to conduct self-evaluations. Boards interested in using this evaluation tool should visit the TBI website at http://theboardinstitute.com/board-risk-meter/.

Learn more at
www.protiviti.com/boardriskoversightmeter