VOLUME 6, ISSUE 8

protiviti®
Face the Future with Confidence

The Bulletin

Protiviti's Review of Corporate Governance

So, You've Implemented ERM? Take Another Look

Now that the Committee of Sponsoring Organizations of the Treadway Commission (COSO) has finalised its *Enterprise Risk Management — Integrating with Strategy and Performance* framework,[1] it's time for companies to take a fresh look at their risk management. While the concepts in the updated framework aren't really new, the emphasis given them is markedly different. The focus is now on what's most important in maximising the value contributed by enterprise risk management (ERM).

The Status Quo for ERM

Notwithstanding the availability of various risk frameworks, including COSO's original ERM framework published in 2004 and *ISO 31000: 2009, Risk Management*,[2] the business motivation behind ERM wasn't sufficiently clear until the 2007–2008 financial crisis. Once the collective weight of excessive risk-taking almost took down an entire industry, triggering hundreds of bank failures, significant taxpayer-funded bailouts and a severe global recession, regulators took notice. Boards began asking tougher questions. CEOs began looking for ways to focus their risk dialogue with directors. The "black swan" concept became real.

The lessons from the crisis demonstrated the vital importance of several key elements to effective risk management. For example, a fully engaged board and a bought-in CEO create the necessary "tone at the top." Other key elements include effective risk governance, a culture that enables open risk dialogue and transparency, a compensation structure that balances short- and long-term interests, and, most important, a management team able to act decisively in a contrarian manner when warning signs of danger are evident.

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

[2] *ISO 31000:2009, Risk management — Principles and guidelines*, International Organization for Standardization, available at www.iso.org/iso-31000-risk-management.html.

Since the 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; and (3) how do we know? In responding to these three questions, executive management and boards of some companies have made progress in differentiating critical enterprise risks — the top risks that can threaten the company's strategy, business model or viability — from the risks associated with normal, ongoing, day-to-day business operations. The increased focus on critical enterprise risks, as well as emerging risks, in the C-suite and boardroom, ensures that the organisation is targeting attention on the vital few risks rather than the trivial many.

In addressing the three questions, many companies have designed processes with key objectives and expected outcomes, such as those illustrated in the table below:

The Current State of ERM: Three Key Questions

	Do we know what our key risks are?	Do we know how they're being managed?
	Key Objectives: • Delineate critical enterprise risks • Identify emerging risks in a timely manner • Provide sufficient visibility to ongoing business risks	**Key Objectives:** • Establish accountability for results in addressing: — Critical enterprise risks — Emerging risks • Establish and clearly communicate risk tolerances and limits • Provide transparency as to sources of assurance for ongoing business risks
	Expected Outcomes: • Focused board and executive management dialogue • Organisation enabled to respond more in a timely manner to emerging issues	**Expected Outcomes:** • Clarity as to responsibility and accountability for managing risk • Escalation protocol to engender confidence in timely reporting of: — Breaches and near-breaches of risk tolerances and limits — Other significant issues warranting attention
How do we know?	• Effective criteria for assessing risk • Defined risk assessment process for identifying and prioritising risks	• Transparency as to risk ownership • Effective risk reporting protocol
	• A repeatable process for identifying, prioritising, mitigating and monitoring the most critical risks	

In summary, the issuance of the original COSO ERM framework in 2004, dramatic risk management breakdowns since that time, and the increasing complexity of the business environment have driven companies and their leaders to upgrade their risk management.

Is It Enough?

Yes, companies have made progress, and the processes they've implemented serve a worthwhile purpose. But is the status quo sufficient to meet the challenges expected over the next five to 10 years?

Consider the results of a recent survey in which only about a quarter of almost 600 executives across the world describe their risk management as "mature" or "robust." Furthermore, many organisations are struggling to integrate their risk management processes with strategic planning, are experiencing pressure from the board of directors to strengthen risk oversight, and are facing barriers that are impeding progress in maturing risk management processes.[3]

What do these results mean? Ask yourself the following questions:

- **Will our ERM approach help us to identify strategic errors in time?** The most recent study[4] of this nature that we could find noted the following:

  > Of U.S. public companies with at least $1 billion in enterprise value as of January 1, 2002 (1,053 in total), 81 percent of the companies experiencing the most dramatic losses of enterprise value over the ensuing 10-year period ending December 31, 2011, incurred those losses as a result of major strategic blunders (e.g., new product or new market failures, flawed mergers and acquisitions, and untimely responses to dramatic shifts in major enterprise value drivers, such as a major input cost).

  The study was based on the premise that all the occurrences contributing to the loss should have been anticipated. But they weren't.[5]

  The Implication: For many companies, ERM is more focused on operational, financial and compliance issues than on strategic issues; therefore, ERM cannot contribute to the management of strategic risk. The speed of risk and change demands more. Is your ERM approach integrated with strategy-setting?

- **Is our organisation able to recognise the signs of disruptive change, and is it agile and resilient enough to adapt to change?** Over time, it has become clear that the half-life of business models is compressing. Powerful megatrends have emerged that can disrupt established business models more quickly than ever, not the least of which are the continued advances in digital technologies. To stay ahead of the disruption curve, business leaders must quickly discern the vital signs of change in the marketplace.

  The importance of this point is reinforced by a survey of some 735 C-level executives and directors across the globe regarding the risks their organisations face.[6] According to the survey results, two of the top risks for 2017 are:

  – The organisation's culture may not sufficiently encourage timely identification and escalation of significant risk issues.

[3] *2017 Global Risk Oversight Report*, by Mark S. Beasley, Bruce C. Branson and Bonnie V. Hancock, jointly commissioned by the Association of International Certified Professional Accountants and North Carolina State University's ERM Initiative, June 2017, available at www.cgma.org/resources/reports/2017-global-risk-oversight-report.html.

[4] "The Lesson of Lost Value," by Christopher Dann, Matthew Le Merle and Christopher Pencavel, *Strategy+Business*, November 27, 2012, available at www.strategy-business.com/article/00146?gko=f2c51.

[5] We recognise that a more recent study period might reflect different results. For example, the 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, so 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 and customer expectations. Whatever the actual percentage, we believe it to be significant.

[6] *Executive Perspectives on Top Risks for 2017*, Protiviti and North Carolina State University's ERM Initiative, available at protiviti.com/toprisks.

– Resistance to change may restrict the organisation from making necessary adjustments to the business model and core operations.

The cultural issues surrounding the escalation of top risk concerns combined with a lack of organisational resiliency can be lethal in an uncertain and rapidly changing business environment.

The Implication: What good is ERM if it isn't helping organisations position themselves as early movers in these dynamic times of disruptive change? After all, it's a digital age where big data technologies, user-driven visualisation tools, digitisation opportunities and cloud deployment models are putting capabilities in reach that were mere theory 10 years ago. Is your organisation exploiting these opportunities to create early alert reporting?

- **Will our CEO "dance until the music stops"?** Just prior to the advent of the financial crisis, the CEO of a major global bank was asked about the risks his bank was taking in the U.S. subprime mortgage market. The CEO replied:

  "When the music stops, in terms of liquidity, things will be complicated. But as long as the music is playing, you've got to get up and dance. We're still dancing."[7]

  Yes, 20/20 hindsight is golden. But there are three reasons why this quote is the stuff of legends. First, the CEO is implying that it doesn't matter what the warning signs posted by the risk management function say. Second, the CEO thought he knew how to time an exit from a highly risky environment in which his organisation was deeply invested and that he was willing to stay in the market as the music played on. More important, it illustrates how difficult it is to exit a market that, at the time, is generating significant revenue and profits. Call it an emotional investment in the existing business model, an unshakable bias in favor of sustaining that model or just plain near-sighted short-termism, the consequences included a massive taxpayer-funded bailout.

  The Implication: How disciplined is your organisation in evaluating risk and return in its decision-making versus blindly following the herd? Is your ERM approach contributing to the appropriate discipline?

- **Do we seek out what we don't know? Are we prepared for a surprise?** Stuff happens. This is *the* lesson from the financial crisis. It was learned again in the Japanese tsunami in 2011. The point is clear: No organisation or brand on the planet is immune to the risk of surprise. So, the question is: What "unknown unknowns" lurk in the external marketplace or are embedded within the organisation's processes that could impair reputation or erode brand image?

  The Implication: How prepared is your organisation to respond to the occurrence of a high-impact, high-velocity and high-persistence risk event? Is ERM focusing your company's preparedness for the unexpected?

- **Is everyone competing for capital and funding with rose-colored 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? Are these decisions carried out on a risk-informed basis?

  The Implication: Resource and budget allocations needn't be a grabfest. There should be a systematic process to drive such allocations to their highest and best use for the enterprise as a whole, consistent with its risk appetite. Is your ERM approach facilitating such a process?

[7] "Citigroup's Chuck Prince wants to keep dancing, and can you really blame him?", *TIME* magazine, July 10, 2007, available at http://business.time.com/2007/07/10/citigroups_chuck_prince_wants/.

Yes, companies have made progress, but the risk management methodologies in play for most businesses today were developed before the turn of the century. In effect, risk management is often an "analogue approach" being applied in what is now a digital world. More importantly, if ERM is a stand-alone process, it is suboptimal.

Bottom line, more needs to be done to elevate risk management to help organisations face the dynamic realities of the 21st century. To keep pace, ERM solutions need to leverage the advances of digital, cloud, mobile and visualisation technologies; exponential growth in computing power; and advanced analytics to embed deeper and more insightful risk information in strategy-setting, performance management and decision-making processes.

COSO's Updated ERM Framework Could Alter the Conversation

In initiating the project to update its ERM framework, COSO saw opportunities to achieve clarity on several fronts. The updated framework recognises the increasing importance of the interconnection of risk, strategy and enterprise performance — particularly in conjunction with making important decisions. It begins with an underlying premise that every entity exists to provide value to 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 appetite. The term "uncertainty" is defined as not knowing how or if potential events may manifest themselves in the context of achieving future strategies and business objectives. "Risk" is considered the effect of such uncertainty on the formulation and execution of the business strategy and the achievement of business objectives.

The challenge for management and the board of directors is to evaluate how much uncertainty — as well as how much risk — they are preparedand able to accept in executing the strategy and pursuing the organisation's performance goals. Therefore, ERM is all about balancing risk and reward in creating value. Achieving that balance leads to an emphasis on protecting enterprise value as well as enhancing it.

The framework is principles-based, meaning it introduces five interrelated components and outlines 20 relevant principles arrayed among those components. The framework is a significant improvement over its 2004 counterpart, as its structure offers a benchmarking option for companies seeking to enhance their ERM approach. The framework focuses on integrating ERM with the core processes that matter; its subtitle says it all — "Integrating with Strategy and Performance." Its concept of integration is embodied within its 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."

If a company implements a stand-alone process, it may be worthwhile and useful, but it is not ERM as COSO defines it. There are four themes that are vital to effective integration of ERM:

Implementation with strategy. COSO elevates the discussion of strategy, risk and risk appetite by asserting 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. In addition, the board of directors and executive management need to define the enterprise's risk appetite in the context of creating and preserving value and consider how the strategy works in tandem within that risk appetite.

Integration with performance. COSO makes it clear that risk reporting is not an isolated exercise. In integrating risk with performance, COSO defines "tolerance" as the "boundaries of acceptable variation in performance related to achieving business objectives." While risk appetite is strategic and broad, tolerance is operational and tactical. Operating within acceptable variations in performance provides management with greater confidence that the entity remains within its risk appetite; in turn, that provides a higher degree of confidence that business objectives will be achieved in a manner consistent with the enterprise's mission, vision and core values.

Lay a strong foundation with risk governance and culture. Internal pressures can lead to unmanageable bias, flawed decisions, and irresponsible and/or illegal behaviour. They are 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. Therefore, the board and CEO must be vigilant in ensuring that pressures within the organisation are not incenting unintended consequences. That is why COSO asserts that strong risk governance and culture are essentials.

Tie risk considerations into decision-making processes. COSO defines "relevant information" as information that facilitates informed decision-making. The more that information contributes to increased agility, greater proactivity and better anticipation of changes to the enterprise in its decision-making, the more relevant it is; consequently, the more likely the organisation will execute its strategy successfully, achieve its business objectives and establish sustainable competitive advantage. Risk reporting encompasses information required to support and enhance management decision-making at all levels as well as enable the board to fulfill its responsibilities.

Every organisation is different according to its industry, strategy, structure, culture, business model and financial wherewithal. From a practical standpoint, companies can implement the COSO framework by using it to evaluate their current ERM approach. As they do so, they will be able to address the above elements of ERM.

Three Keys to Advancing ERM

In using the principles provided by the COSO framework to advance ERM within the organisation, we suggest organisations focus on the three keys discussed below.

Key #1: Position your organisation as an early mover. When a market shift creates an opportunity to deliver enterprise value or invalidates critical assumptions underlying the strategy, it is in an organisation's best interests to recognise that insight and act on it as quickly as possible. As noted earlier, it makes sense to enhance the enterprise's ability and discipline to recognise changing market realities and act decisively in revising strategic and business plans in response to those realities.

The financial crisis made it easier to recognise the value of time advantage in securing positioning as an early mover. That advantage is attained when the organisation 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. Organisations committed to continuous improvement and able to embrace breakthrough change are more apt to be early movers.

Following is a table illustrating characteristics typical of an early mover:

Attributes of an Early Mover

***RECOGNISES** opportunities and risks, quickly discerning which ones are most critical*	• Understands critical strategic assumptions • Applies contrarian, scenario-analysis capabilities • Conducts competitive intelligence capabilities with early alert mechanisms • Distills information in a timely manner
***REACTS** to opportunities and warning signs to position the organisation early in the game*	• Fosters a culture that is sensitive to changing market realities • Stimulates managerial intuition and ingenuity • Manages the bias, short-termism and emotional investment that can create potentially lethal organisational "blind spots"
***REFLECTS** on experiences to ensure continuous learning*	• Encourages admission of errors and misses, and learns from them • Internalises and converts lessons learned into improvements

The following question applies 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 looking at the emerging risk of an outdated strategy? Time advantage enables proactive opportunity pursuit. In essence, companies functioning as early movers see change on the horizon more often as potential market opportunities than potential crises. They recognise that clinging to the status quo can be dangerous.

Key #2: Address the challenges of risk reporting. The business environment features rapid advances in and applications of digital technologies that are altering business models, improving business processes and enhancing the customer experience. 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. For most organisations, today's risk reporting falls short of that objective.

To impact decision-making, risk reporting must address three questions:

1. Are we riskier today than yesterday?

2. Are we going into a riskier time?

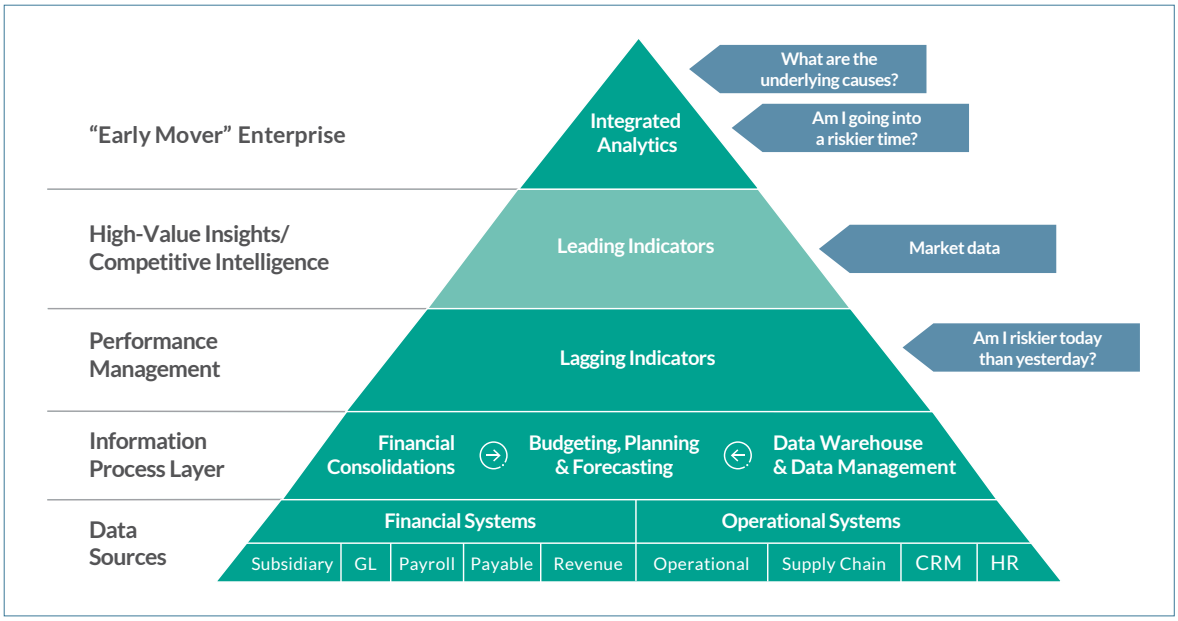
3. What are the underlying causes?

Risk reporting faces multiple challenges. Traditional methods of risk measurement tend to generate information that is difficult to aggregate and interpret across multiple types of risks, lines of business and geographies. Traditional risk reporting lacks transparency into the underlying data, making it difficult to assess the direction and speed of risk, understand the drivers of risk, consider risk in the context of enterprise strategy, and enable a robust risk appetite dialogue. As a result, the amount of manual effort required to collect data from multiple sources, update metrics and create PowerPoint presentations to deliver what decision-makers require is often excessive. "Dynamic" is certainly not the word one thinks of when describing the process.

To combat today's rapidly changing environment, companies need a more dynamic, comprehensive and comprehensible snapshot of their organisation's risk profile so that risk officers, senior executives, board members and decision-makers at all levels of the organisation become more confident that they not only understand the critical risks, but can also act quickly when risk levels are rising or falling with knowledge of the consequences of their decisions. A more agile and nimble process would enable value-added risk analysis, resulting in further insight for decision-making.[8]

Simply stated, risk reporting is often not actionable enough to support decision-making processes. Until it is designed to answer the above three questions, it won't. And once it does, it elevates the organisation up the enterprise information hierarchy from relying on lagging retrospective indicators so typical of most performance management systems to incorporating a more balanced family of measures that includes leading indicators and advanced analytics to drive value-added insights, competitive intelligence and early-mover positioning (see schematic below).

• • • *The Enterprise Information Hierarchy*

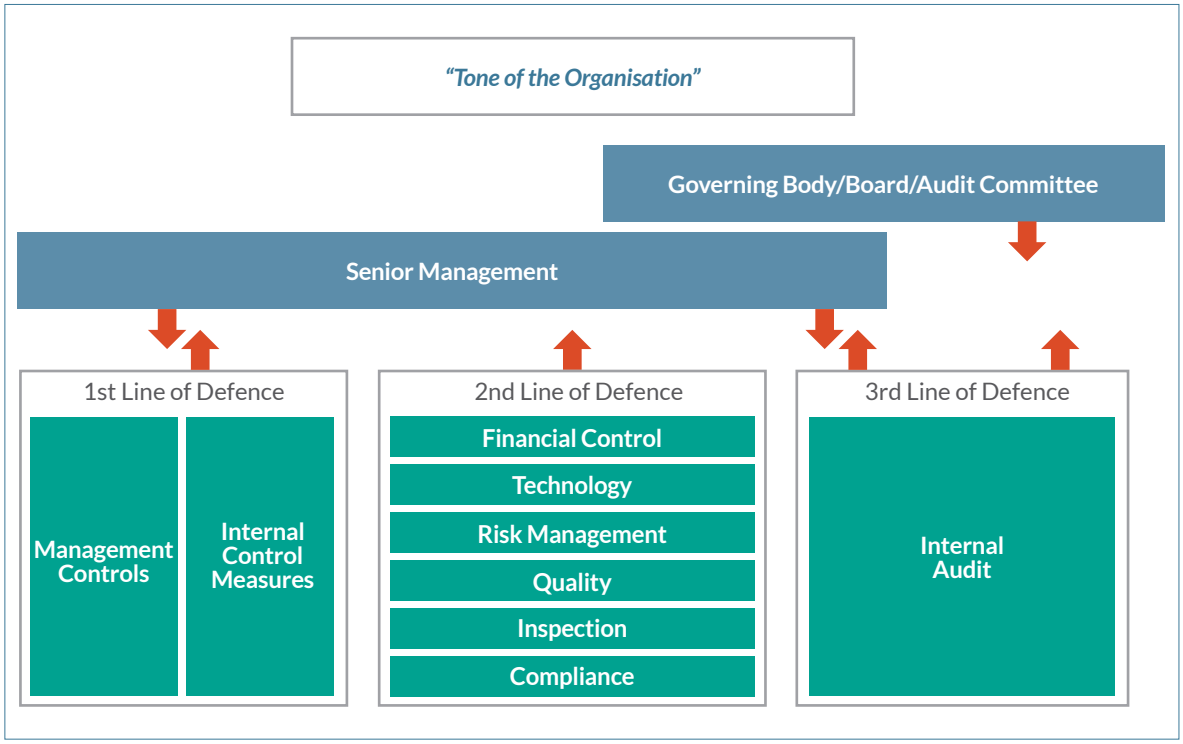


The integration of performance management and risk management on matters of strategic importance is where corporate performance management systems often fail. As a result, the organisation is unable to monitor the vital signs that help anticipate emerging opportunities and risks. Effectively integrated with performance management, risk reporting is a key to evolving ERM from a "risk listing" process to a "risk-informed" decision-making discipline.

[8] For an example of an innovative approach to risk reporting made possible by combining an effective, efficient and customised risk management tool with leading data visualisation technology, see discussion of The Protiviti Risk Index™ at protiviti.com/US-en/insights/protiviti-risk-index.

Key #3: Preserve reputation by maximising your lines of defence. How do organisations safeguard themselves against reputation-damaging breakdowns in risk and compliance management? The long-standing lines-of-defence framework emphasises a fundamental concept of risk management: *From the boardroom to the customer-facing processes, managing risk, including compliance risk, is everyone's responsibility.* A widely accepted view of the lines-of-defence model involves three lines of defence in which the business unit management and process owners whose activities give rise to risk comprise the first line, independent risk and compliance functions are the second line, and internal audit is the third line, as the schematic below illustrates.

• • • *The Lines of Defence*



The tone of the organisation — the collective impact of the tone at the top, the tone at the middle and the tone at the bottom on risk management, compliance and responsible business behaviour — enables the three lines of defence depicted above to be effective. Yes, tone at the top is vital. But when leaders communicate the organisation's vision, mission, core values and commitment to appropriate behaviour, what really drives behaviour is what employees see and hear every day from the managers to whom they report. The proper tone has a significant influence on the organisation's risk culture, which, in turn, affects the functioning of the three lines of defence.

Arguably, the final line of defence from the standpoint of the shareholders is senior management and the board of directors. Under the board's oversight, executive management balances the inevitable tension between business unit managers and process owners (first line of defence) and the entity's independent risk management functions (second line of defence) by ensuring that neither of these two activities are too disproportionately strong relative to the other.

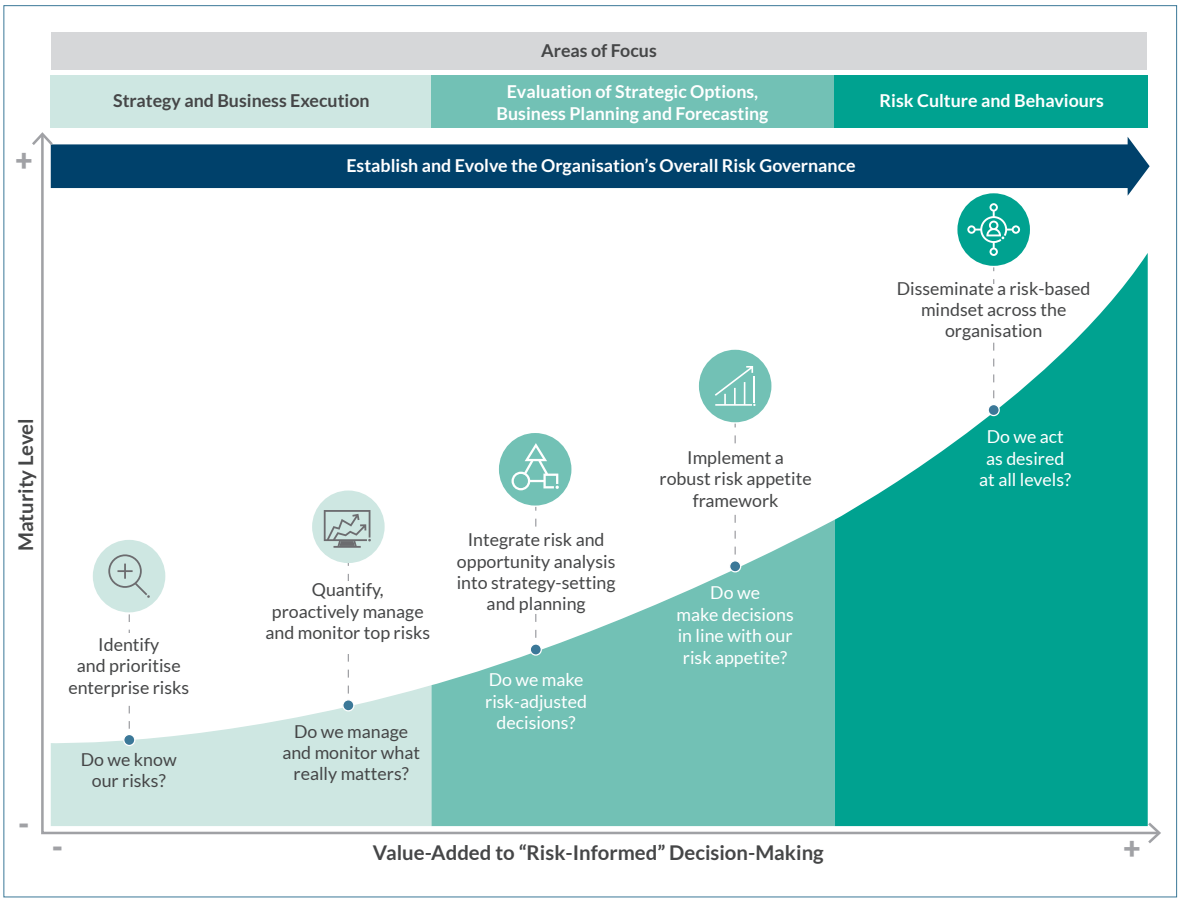
Top management acts on risk information on a timely basis when significant issues are escalated and involves the board in a timely manner when necessary.

The lines-of-defence framework offers a powerful line of sight for companies seeking to strike the appropriate balance between creating and protecting enterprise value and avoiding irresponsible business behaviour that can impair reputation and brand image.[9]

Where Should the Organisation Be on the ERM Journey Continuum?

ERM is a journey toward a new paradigm of risk-informed decision-making, enabled by a strong risk culture and integration with strategy and performance. Companies must decide where they want their ERM approach to be along the maturity continuum. Examples of possible options for executives to consider are shown below:

• • • *The ERM Journey Continuum*



At the far left of the ERM Journey is "identify and prioritise enterprise risks." That option, along with some migration to the second option — "quantify, proactively manage and monitor top risks" — represents the current state of most ERM implementations, as we described at the beginning of this issue of *The Bulletin*. That current state essentially answers the three questions: What are the risks, how are they being managed, and how do we know?

[9] See an elaboration of the lines-of-defence framework in Issue 4 of Volume 5 of *The Bulletin*, "Applying the Five Lines of Defense in Managing Risk," Protiviti, September 2013, available at protiviti.com/OM-en/insights/bulletinv5-i4. So far as we have been able to determine, Sean Lyons is the first author to have broadened the focus of the traditional three lines-of-defence concept in a Conference Board paper dated October 2011. Mr. Lyons' approach is different from the one we outline both above and in the referenced issue of *The Bulletin* and is available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1938360.

However, the second option moves beyond the current state of the art. It involves in-depth risk analysis and quantification, including root-cause analysis, what-if scenario analysis, data and predictive analytics, data modelling and simulations, and stress testing. Such analysis drives focused risk responses, enhanced risk governance and more robust risk reporting, monitoring and early warning capabilities. It begins to elevate ERM to a strategic level.

As noted on the ERM Journey, a third option is to integrate risk and opportunity analysis into strategy-setting and execution to facilitate a clearer understanding of major risks in strategy- and objective-setting and leverage enhanced capabilities to anticipate, adapt and respond to change. Exponential increases in computing power are enabling practical applications of Monte Carlo quantification techniques to consider all possible outcomes of multiple decisions and scenarios so that management can assess the impact on the enterprise's risk profile, allowing for better decision-making in uncertain conditions. It also enables more effective dialogue during decision-making processes about uncertainties and vulnerabilities relating to strategic assumptions and targets, as well as visualisation of management's instincts in useful ways.

Implementing a robust risk appetite framework is the fourth option. Such a framework:

- Identifies risks that should be accepted or rejected in strategy-setting and execution;
- Defines strategic, operational and financial parameters within which the business should operate; and
- Factors the defined parameters into performance management and decision-making in the form of tolerances.

Although a company can develop a risk appetite framework at any time, there is a presumption that such a framework is more meaningful when based on risk management capabilities made possible through the other options on the ERM maturity continuum.

The last option along the ERM Journey is to disseminate a risk-based mindset across the organisation. While this too can be attempted at any time, it is more influential in terms of shaping risk culture when predicated on the capabilities provided by the other options. It sets a stronger tone of the organisation regarding risk, enables more effective risk escalation to senior management and/or the board, and enhances the emphasis on balancing entrepreneurial and control activities.

The five options provided here are intended to be illustrative. They convey that there is no one-size-fits-all approach to implementing ERM. The question is, where does your organisation belong on this ERM Journey Continuum and how does it apply the COSO framework to get there?

Summary: Time for a Fresh Look?

Forget about ERM being an overlay on the core business processes that matter. Yes, that may be a common fear, but if senior executives are concerned about it, their advisers either don't understand what ERM is — given how COSO has defined it — or they are asking the wrong questions.

ERM is not a stand-alone process; it is an approach and discipline to be embedded within existing management processes. The relationship of ERM to the processes the CEO values most can be compared to the contribution of salt, pepper and other seasonings to a sumptuous meal. Without the appropriate seasoning, even a substantive meal can be left lacking. Sometimes a meal needs that "special sauce."

So we end as we began: Is it time to take another look at your risk management? Simply stated, risk management for most companies does not yet fully leverage the powerful tools that have emerged in the 21st century — increased computing power, digitisation, advanced analytics, mobile computing and data visualisation techniques, among others — and the capabilities they make possible. Until it does,

management can't get serious about tying ERM into strategy, performance and decision-making. The whole idea is to enhance the odds of the organisation achieving its objectives by enabling it to become more adaptive in the face of an increasingly volatile, complex and uncertain world. As a result, management and the board can face the future more confidently. If that idea is appealing, are you ready to take another look?