VOLUME 6, ISSUE 10

protiviti®
Face the Future with Confidence

The Bulletin

Protiviti's Review of Corporate Governance

A Risk-Informed Approach to Enterprise Risk Management

Following the September 2017 release of *Enterprise Risk Management — Integrating with Strategy and Performance*[1] by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), Protiviti published an issue of *The Bulletin* encouraging companies to take another look at their enterprise risk management (ERM).[2] Then, in October, Protiviti's ERM Center of Excellence, together with the COSO chairman and a member of the COSO Advisory Council, conducted a webinar to discuss the importance of the updated framework and its relevance to companies in today's business environment.[3] And now, in this latest installment of *The Bulletin*, we explore the ERM topic once again — this time examining how a "risk-informed" perspective can advance the maturity of ERM in an organisation.

[1] *Enterprise Risk Management — Integrating with Strategy and Performance* is available at www.coso.org/Pages/default.aspx.

[2] "So, You've Implemented ERM? Take Another Look," *The Bulletin*, Volume 6, Issue 8, Protiviti, 2017: www.protiviti.com/US-en/insights/bulletin-vol6-issue8.

[3] "Deriving Value from the Updated COSO ERM Framework," Protiviti webinar, October 12, 2017. View the recording at: www.protiviti.com/US-en/insights/deriving-value-updated-coso-erm-framework.

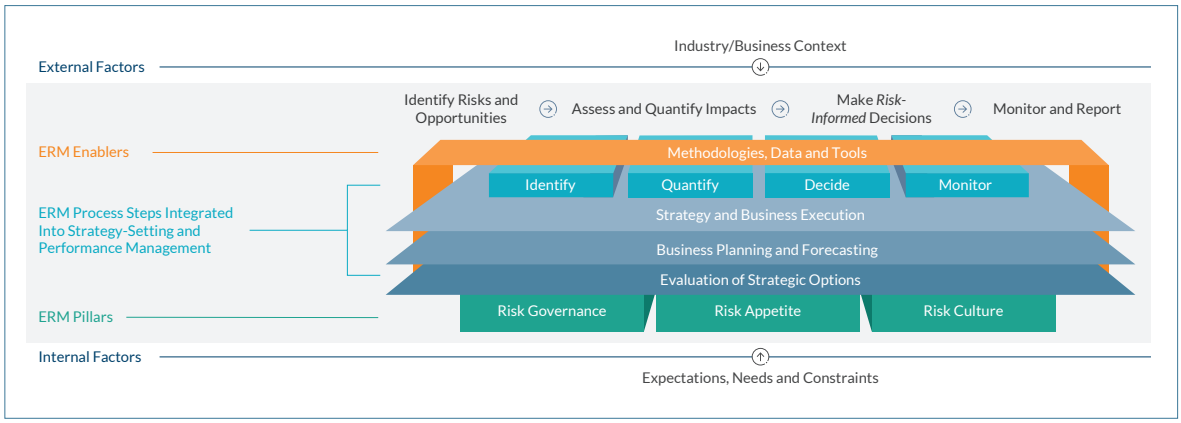
The Importance of a Risk-Informed Perspective

In advancing ERM capabilities, we believe a risk-informed approach lies at the very heart of what effective ERM contributes to an entity's strategy-setting and execution cycle. Once integrated into core business processes, ERM provides management and the board with relevant information on risks and opportunities as they fulfill their respective responsibilities. As executives and directors encourage embedding more formal and timely considerations of risk in decision-making and performance review processes, better decisions in the pursuit of business objectives result.

Properly structured, this approach supports the development and evolution of a risk management programme that is:

- *Strategic* in considering the impact of risk on strategy and performance;
- *Balanced* in measuring both risks and opportunities;
- *Integrated* with strategy-setting, planning and business execution; and
- *Customised* to reflect organisational business needs, stakeholder expectations and cultural attributes.

Protiviti's Risk-Informed Approach



We have taken license to visualise in the above schematic the elements of a risk-informed approach. As can be seen, it embraces the concept of integration embodied in the recently updated COSO framework, which focuses on integrating ERM with strategy, performance and decision-making supported by strong risk governance and culture. It also is impacted by, and is sensitive to, external and internal factors. We discuss our approach in more detail below.

The integration of ERM with strategy-setting and business planning can change the conversation about ERM. This approach can help organisations open their eyes to the future, reduce surprises and be more prepared to face disruptive change and uncertainties.

Key Components of a Risk-Informed Approach

There are several important components that support decision-making from a risk perspective.

Integration into strategy-setting and performance management

An ERM approach can successfully support risk-informed decisions only if risk identification, quantification, management and monitoring activities are integrated into (a) the *evaluation and selection of strategic options,* (b) the *development of strategic and business plans,* and (c) the *execution of those plans.* This focused integration allows management and the board to make relevant decisions based on "risk-return" considerations. Without it, ERM remains an appendage, which reduces its impact.

The three pillars of ERM

Three pillars — *risk governance, risk appetite* and *risk culture* — are emphasised in the COSO framework and form the foundation of an effective ERM system:

- **Risk governance:** The governance structure reflects the oversight and accountability for risk issues, from individual roles and responsibilities to management committee structures and oversight by the board of directors. The design and implementation of the risk governance structure, including policies, reporting and escalation practices, impact ERM and risk-informed decision-making.
- **Risk appetite:** A risk appetite statement articulates the risks an organisation is willing to undertake in the pursuit of business objectives. It presents an opportunity for management to clarify to the board and the rest of the organisation the nature and extent of acceptable risks in executing the strategy. We agree with COSO that there is no standard approach to articulating risk appetite. COSO's ERM framework offers guidance on how management and the board can express the parameters within which to operate the business that are consistent with Protiviti's long-standing guidance and our supporting white paper on the appropriate levers of enterprise risk.[4]
- **Risk culture:** The keystone that holds things together, culture provides a source of strength or weakness for the organisation. An actionable risk culture helps balance the inevitable tension between (a) creating enterprise value through the strategy and driving performance on the one hand and (b) protecting enterprise value through risk appetite and managing risk on the other hand. In effect, risk culture balances the push between strategy and risk appetite.

These three pillars lay the foundation for how ERM works in enhancing decision-making. An organisation should customise these pillars based on its industry, its strategy for creating enterprise value, the core values of its directors and management, the regulatory environment, and other factors. However, the underlying principles should remain consistent as this foundation sets the tone, frames the boundaries and establishes the policies necessary to put effective risk management into practice.

ERM enablers

ERM enablers, including **methodologies, data and tools,** play a critical role in a "risk-informed" approach. Based on our experience, objective and measurable information about risks and opportunities leads to better decisions because it enables more effective dialogue about uncertainties associated with performance targets and variations from targets. It also facilitates — through the aggregation of different risk exposures — management's understanding and monitoring of the overall risk profile. We refer to these components as ERM enablers for two

[4] *Defining Risk Appetite — Early Mover Series: Integrating Corporate Performance Management and Risk Management*, Protiviti, 2012: www.protiviti.com/UK-en/insights/wp-early-mover-series-integrating-corporate-performance-management.

reasons. First, they allow management and the board to formulate a shared view about the risk profile, as well as acceptable performance variability. Second, they improve resource allocation through higher-quality risk-return analyses.

Internal factors and external factors

Internal factors and external factors influence ERM as well. The former drives expectations, needs and constraints, while the latter defines the industry and business context.

- **Internal factors** vary by organisation but are influenced by the risk culture. They include the expectations from the top of the organisation, the established governance structure, business model complexity, and the availability and quality of resources and data.
- **External factors** may include known and emerging market trends, industry regulations, listing requirements, external stakeholder expectations, and unexpected events. They may serve as either shortcuts or roadblocks in the path to creating an effective ERM programme. External factors also create risk, requiring enhancements in risk management capabilities continuously over time.

An effective risk-informed approach must navigate both internal and external factors, whether they facilitate or challenge the organisation as it advances along its ERM journey.

All the components described above play both individual and collective roles in an ERM journey that aims to move an organization from a compliance, check-the-box, risk-listing mindset to a risk-informed approach that helps the business create and preserve enterprise value proactively.

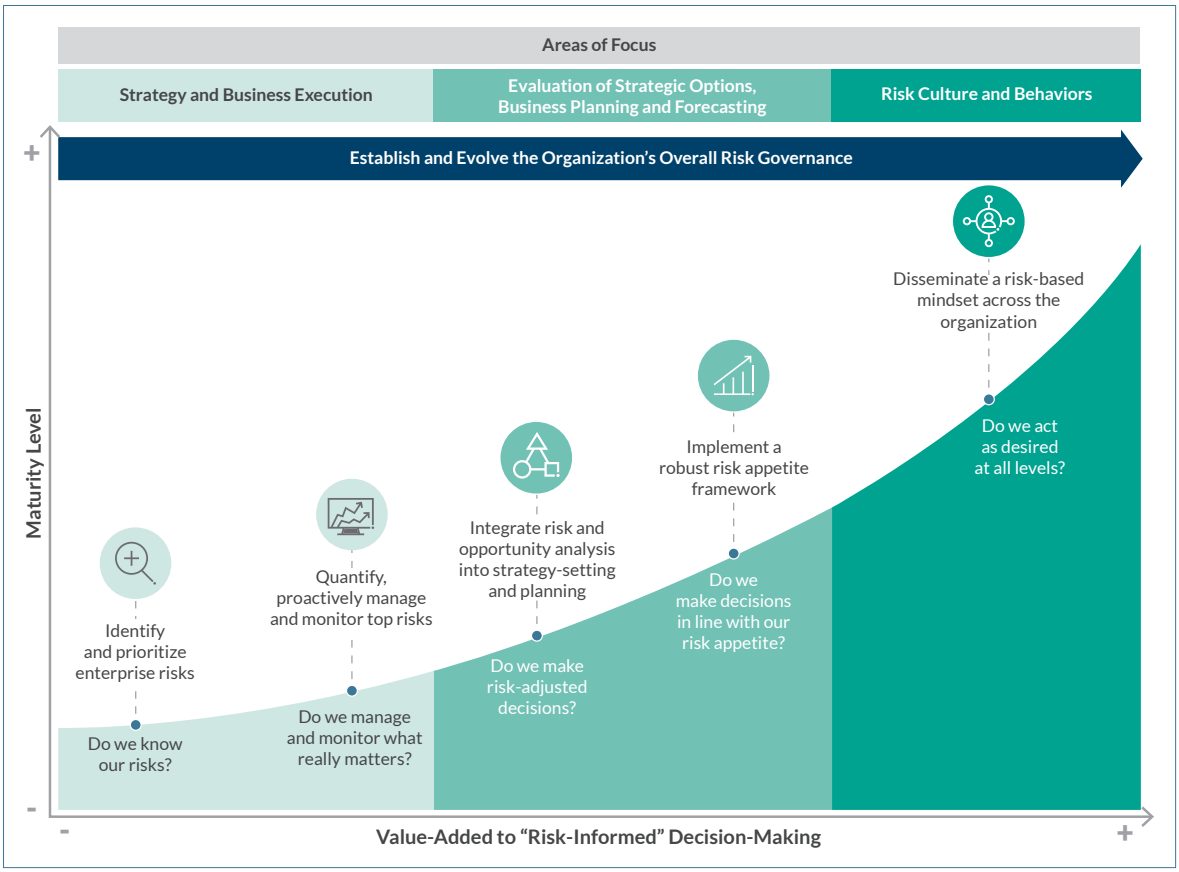
ERM Journey to Risk-Informed Decision-Making

Each company's ERM programme is influenced by its unique culture, strategy, business goals and financial wherewithal. Accordingly, ERM is a journey because it is evolving constantly in the face of changes in the business environment.

As there is no one-size-fits-all solution to implementing ERM, one of the key benefits of a risk-informed journey in approaching it is that it can be tailored to fit the existing maturity, risk culture and risk management needs of any organisation. That said, the final goal remains the same: improving the entity's capability to add increasing value to decision-making as it seeks to achieve its business objectives.

Viewing ERM as a journey helps entities identify their current state and envision their next steps as the environment changes. As long as the goal is clear, advancing toward it should be considered progress. Likewise, as long as the environment changes, the journey never ends.

• • • *The ERM Journey Continuum*



A critical step in a risk-informed approach is to understand the organisation's current state (i.e., where it is along the journey) so that management can evaluate how to advance. The ERM Journey Continuum, illustrated above, starts with risk identification and prioritisation and progresses to the rigorous dissemination of the entity's risk culture across all levels of the organisation. As the organisation takes each step along the ERM journey, the aggregate value added to risk-informed decision-making increases until ERM is implemented in a way that truly influences strategic thinking and execution in setting and achieving business objectives.

Implementation of each initiative (or "building block") depicted in the continuum need not be sequential. Organisations can embrace building blocks at different points during their ERM journey. For instance, an entity might first implement a risk appetite framework before piloting a risk and opportunity analysis integrated into strategic planning. Or, it may decide to launch a risk culture programme before pursuing other ERM initiatives. As noted earlier, each organisation's journey to advancing ERM maturity is different, depending on the priorities and needs agreed upon by executive management and the board.

Following are some observations about the five initiatives depicted in the continuum:

- **Identify and prioritise enterprise risks:** While it seems logical to begin with a risk identification and prioritisation capability — and many organisations do, in fact, initiate their ERM journey in this way — implementing this initiative does not usually require a sophisticated risk culture and approach. Risk identification and prioritisation, undertaken on a stand-alone basis, may remain disconnected from strategy-setting and performance management, and often is. As a result, this

initiative — standing alone — might not be sufficient to support a risk-informed decision-making system. If relegated to a check-the-box, risk-listing exercise, it loses effectiveness over time as the pace of change accelerates.

- **Quantify, proactively manage and monitor top risks:** Integrating more sophisticated risk quantification and monitoring capabilities into the day-to-day activities of the business in executing the strategy can help management aggregate relevant risks into a composite risk profile. Also, it provides more granular information about aggregate risk exposure as well as the costs and benefits expected from alternative risk responses and scenarios. This initiative implies the implementation of more sophisticated tools and techniques that support performance management and related decisions when executing the strategy, leading to a higher level of ERM maturity.
- **Integrate risk and opportunity analysis into strategy-setting and planning:** This initiative focuses on the evaluation and selection of strategic options based on their relative risks and rewards. It enables value-added insights, competitive intelligence and early-mover positioning using leading indicators, early warning capabilities, proprietary models and advanced analytics linked to critical strategic assumptions and targets. Most important, it helps to foster more effective dialogue during decision-making processes and improved anticipation of future exposures and vulnerabilities.
- **Implement a robust risk appetite framework:** Risks are inherent in setting business objectives and in every strategy for achieving those objectives, whether the organisation expresses them explicitly or not. A clear risk appetite statement aligned with the strategy is vital to ERM because an effective risk-informed approach focuses the entity on managing enterprise risk within the bounds of its stated appetite. Thus, risk appetite is a strategic tool that offers a context for addressing strategic decisions. When pushed down into the organisation in the form of risk tolerances tied to performance objectives, it facilitates day-to-day decisions and actions by managers on the front lines and in the support functions that consider the entity's overall appetite for risk, as agreed by executive management and the board. In turn, it helps the organisation avoid the assumption of excessive risk exposures without the executive team's and the board's knowledge.
- **Disseminate a risk-based mindset across the organisation:** By cultivating and supporting a robust risk culture at all levels of the organisation (i.e., including line management and process owners whose activities and decisions create risk), an entity ensures that responsible personnel undertake day-to-day decisions in the pursuit of achieving business objectives in a risk-informed manner that balances risk and opportunity considerations. A risk-based mindset fosters a strong tone of the organisation regarding risk and effective escalation of risk issues to senior management and the board.

The above initiatives illustrate the types of considerations given to advancing ERM as a discipline and framework for elevating risk management to a strategic level. It is not intended to list all initiatives needed to complete a given organisation's road map to implement ERM. The point of the continuum is for organisations to challenge themselves to resist "risk listing" without considering the potential impact to strategy and performance.

Integration With Strategy and Performance Management

For many organisations, an important milestone in the ERM journey is evolving the ERM approach into a valued input and tool for strategy-setting and performance management. In its ERM framework, COSO suggests that organisations consider three dimensions when focusing on strategic risks and their impact on achieving business objectives: (1) assessing the risks arising from the strategy; (2) assessing the risk of the strategy and the organisation's mission, vision and values being out of alignment; and (3) managing the risks to the execution of the strategy and integrating risk with performance.

Below, we summarise examples of integrating ERM with the three core management processes illustrated in the centre of our risk-informed approach schematic introduced earlier:

Management Process	Key Questions Addressed by ERM
Evaluation of Strategic Options	• Are the strategic options the organisation is considering in the pursuit of stated business objectives in line with its vision, mission and core values? • What is the risk-return profile of various strategic options (e.g., initiating capital investments, introducing new products and services, entering new markets, accepting new customers and projects, and forming alliances with new strategic partners)? • Which strategic option is in line with the entity's established risk appetite?
Business Planning and Forecasting	• What risks are embedded in the business plan and forecast? • Given the risks undertaken, is the plan robust enough or too ambitious? • What is the level of resilience in the plan should alternative scenarios — plausible and extreme — occur during the planning horizon? • Which risks to plan execution does the entity need to address during the planning horizon and why?
Strategy and Business Execution	• Is the organisation focused on the risks that are critical to the achievement of its business objectives and strategies? • Are the key risks appropriately measured and monitored? • Are risks managed to ensure they are within the entity's risk appetite? Is corrective action taken to address excessive risks? • Are key risk indicators monitored during strategic execution?

The point is that forward-thinking organisations use ERM to integrate strategy, business planning and key decision-making processes to drive better performance in their quest to achieve business objectives.

Measuring the Success of ERM

At some point, executive management wants to know if ERM success is being measured in some way to ensure it contributes the intended value. Responding to such a deceptively simple request is not easy when there are so many forces, external and internal, shaping the organisation's future and its ultimate success or failure.

If management makes good decisions, how can one know whether the decision would have been different had an effective ERM programme not been in place? On the other hand, if management makes a poor decision, how can one know whether a better decision would have been made had the organisation implemented ERM? Would ERM have made a meaningful difference in the decision-making process? Proof is often elusive on this score.

Some believe that building and sustaining a competitive advantage and producing incremental increases in cash flows and earnings per share are, in themselves, indirect measures of risk management used in this regard include return on investment (ROI), return on equity (ROE) and shareholder value added. Useful nonfinancial measures include customer satisfaction and retention, employee satisfaction and reduced attrition, channel throughput, market share, and brand image.

With respect to success measures directly related to risk management, there are various indicators that companies can use in evaluating the effectiveness of their ERM approach and obtaining insights on its contribution to the organisation's success. Following are some examples:

1. Effective assessments of operational risk to improve preparedness for the unexpected
2. Integration of risk assessment into core management processes
3. An informed and effectively functioning board risk oversight process
4. Timely identification of emerging risks and effective implementation of early warning systems
5. Reduction in performance variability
6. Reduction in the number of risk incidents or near misses
7. Reduction in the cost of capital and improvement in shareholder value
8. Increased risk sensitivity and awareness in the firm's culture

In the digital economy, ERM is a difference maker if it contributes to reshaping strategy in advance of disruptive change. When the fundamentals of the business are about to change, executive management must be prepared to secure "early mover" positioning in the marketplace to capitalise on emerging market opportunities and risks on a timely basis. If executive management and the board recognise this contribution, that alone can be a powerful validation of a risk-informed approach to ERM.

Summary

We believe that a risk-informed approach to ERM is an important differentiator that increases an organisation's chances of success in achieving its strategic objectives and performance goals. Thoughtful ERM programmes help companies anticipate, adapt and respond to change. They also focus management efforts and resources on the risks and opportunities that truly matter in terms of their impact on strategy and performance.

In future issues of *The Bulletin,* we will share more guidance on enhancing ERM programmes and risk management capabilities along the ERM journey.