Board Perspectives: Risk Oversight

COSO ERM – What It Means to the Board

Issue 81

Recently, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) released its updated enterprise risk management (ERM) framework for public exposure and comment. Why is this updated framework important to boards of directors? Below, we summarise a few important takeaways.

COSO's recently issued exposure draft of *Enterprise Risk Management: Aligning Risk with Strategy and Performance* addresses important lessons from the financial crisis of 2008. As we look back, it's still hard to believe that an entire industry was culpable in creating a credit crunch so severe that it triggered an ugly global recession and the need for massive government bailouts.

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 CEO, an open and transparent culture, a compensation structure that balances short- and long-term goals and interests, an understanding of the risk implications of the strategy, and a recognition that critical strategic assumptions can be invalidated by changes in the environment.

COSO emphasises these elements in its updated framework. In this era of disruptive change, directors would be well-advised to ensure that these attributes exist within the organisations they oversee. The reality is clear: To stay ahead of the disruption curve, business leaders must quickly discern the vital signs of change and all related implications for their markets and business models.

The updated framework offers important insights for directors. We explore five of them below.

Identifying risks to the strategy is not enough. Many organisations focus on identifying risks to the execution of the strategy. That's a good thing. However, COSO asserts that "risks to the strategy" is only one dimension of strategic risk. There are two additional dimensions to applying ERM in strategy-setting that can significantly affect an enterprise's risk profile:

- The second dimension is the "possibility of strategy not aligning" with an organisation's mission, vision and core values, which define what it is trying to achieve and how it intends to conduct business. Directors should ensure that the company doesn't put into play a misaligned strategy that increases the possibility the organisation may run askew of its mission and vision, even if that strategy is successfully executed.
- The third dimension to consider is the "implications from the strategy." 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." When overseeing strategy-setting, directors need to consider how the strategy works in tandem with the organisation's risk appetite, and

how it will drive behaviour across the organisation in setting objectives, allocating resources and making key decisions.

In summary, the updated COSO framework asserts that all three dimensions need to be considered as part of the strategy-setting process. Failure to address all three could result in unintended consequences that lead to missed opportunities or loss of enterprise value.

Recognising and acting on market opportunities and emerging risks on a timely basis is a differentiating skill. COSO asserts that an organisation can be viable in the long term only if it is able to anticipate and respond to change, not only to survive, but also to evolve. Enterprise resilience, or the ability to function as an early mover, is an indispensable characteristic in an uncertain business environment.

Therefore, corporate strategies must accommodate uncertainty while staying true to the organisation's mission. Organisations need to exhibit traits that drive an effective response to change, including agile decision-making, the ability to respond in a cohesive manner, the adaptive capacity to reorganise, and high levels of trust and collaboration among stakeholders.

Strengthening risk governance and culture sets the right tone. Risk governance sets the organisation's tone and reinforces the importance of, and establishes oversight responsibilities for, ERM. Culture pertains to ethical values and responsible business behaviours, particularly those reflected in decision-making. COSO asserts that several principles drive the risk governance and culture needed to lay a strong foundation for effective ERM:

- **Fostering effective 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 must possess the requisite skills, experience and business knowledge to provide that oversight. The board should serve as a check and balance on executive management and institutional bias.
- **Recognising the risk profile of the operating model –** 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. The ERM process must take into account the risk profile of the enterprise's operating model.
- **Encouraging risk awareness –** COSO frames desired organisational behaviours within the context of the enterprise's core values and attitudes toward risk. Whether an organisation considers itself risk averse, risk neutral or risk aggressive, COSO suggests that it should encourage a risk-aware culture. Such a culture is characterised by strong leadership, a participative management style, accountability for actions as well as results, embedding risk in decision-making processes, and open and positive risk dialogues. These characteristics integrate risk into the day-to-day business.
- **Demonstrating 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 down into the organisation. This means the tone in the middle must be aligned with the tone at the top so 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. Standards of conduct must be established and evaluated and any deviations from those standards addressed in a timely manner. Open communication and transparency about risk and risk-taking expectations are vital to setting the appropriate tone.
- **Establishing accountability for ERM –** Individuals at all levels of the organisation must be accountable for ERM. Just as important, the organisation 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 organisation through appropriate

incentives and reward systems. The board and CEO must be vigilant in ensuring that pressures within the organisation 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 those for longer-term focused stakeholders (e.g., corporate sustainability targets). Pressures can also arise from substantial change (e.g., changes in strategy, shifts in customer needs affecting sales performance or disruptive change affecting the viability of the operating model).

- **Attracting, developing and retaining talented individuals –** It is important to build the human capital and the talent of individuals in alignment with the needs set by business objectives. Management must define the knowledge, skills and experience required to execute the strategy; set appropriate performance expectations; attract, develop and retain the appropriate personnel and strategic partners; and arrange for orderly succession.

Advancing the risk appetite dialogue adds value to strategy-setting. The institution's risk appetite statement is considered during the strategy-setting process, communicated by management, embraced by the board and integrated across the organisation. 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.

To be useful, risk appetite must be driven down into the organisation. To that end, 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. Operating within acceptable parameters of 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 entity will achieve its business objectives in a manner consistent with its mission, vision and core values.

Monitoring what really matters is essential to effective ERM. The organisation monitors risk management performance and how well the components of ERM function over time, in view of any substantial changes in the external or internal environment. If not considered on a timely basis, change can either create significant performance gaps vis-à-vis competitors or invalidate the critical assumptions underlying the strategy.

Monitoring of substantial changes is built into business processes in the ordinary course of running the business and conducted on a real-time basis. As ERM is integrated across the organisation, embedding continuous evaluations can systematically identify process improvements.

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

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 ERM process, as well as implementing strategies, tactics and success measures for managing and reporting specific financial, operational, technology and other risks.

About Protiviti

Protiviti (**www.protiviti.com**) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit, and has served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. Protiviti and our independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Ranked 57 on the 2016 *Fortune* 100 Best Companies to Work For® list, Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Protiviti is partnering with the National Association of Corporate Directors (NACD) to publish articles of interest to boardroom executives related to effective or emerging practices on the many aspects of risk oversight. As of January 2013, NACD has been publishing online contributed articles from Protiviti, with the content featured on www.nacdonline.org/Magazine/author.cfm?ItemNumber=9721. Twice per year, the six most recent issues of *Board Perspectives: Risk Oversight* are consolidated into a printed booklet that is co-branded with NACD. Protiviti also posts these articles at **Protiviti.com.**

protiviti®
Risk & Business Consulting.
Internal Audit.