

Board Perspectives: Risk Oversight

Principles for Improving Board Risk Reporting

Issue 77

A fundamental underpinning of effective board risk oversight is timely, reliable and insightful risk reporting. Below, we discuss six principles for delivering the focused risk reporting the board needs.

Within many organizations, board risk reporting is a subject of debate. We often hear such statements as “the reports we get are too detailed,” “reports are not actionable or focused on the right issues,” “we’re not sure what the board wants” and, the all-time classic, “we’re not sure the board knows what it wants.” The truth is, these and similar comments may be symptoms of broader issues in an organization.

Key Considerations

Just over five years ago, Protiviti conducted a survey of more than 200 directors regarding the then-current state of board risk oversight.¹ With respect to risk reporting, the survey results noted:

- The most common types of risk reporting received at least annually by boards included a high-level summary of top risks for the enterprise, as a whole, and its operating units; a periodic overview of management’s methodologies used to assess, prioritize and measure risk; and a summary of emerging risks that warrant board attention.

- Among those reports not received annually by most boards are scenario analyses evaluating the effect of changes in key external variables impacting the organization; a summary of exceptions to management’s established policies or limits for key risks; and a summary of significant gaps in capabilities for managing key risks and the status of initiatives to address those gaps.
- Reports not received at least annually were generally received only on an as-needed basis – or not at all.

Since then, we have seen (a) efforts by senior management and risk executives to improve board risk reporting, and (b) some boards acknowledging that the risk reports they receive are improving. Recently, the North Carolina State University ERM Initiative obtained input from more than 20 chief risk officers and other executives leading enterprise risk management efforts at a number of major U.S. corporations serving on the ERM Initiative Advisory Board regarding their board risk reporting practices.² As to be expected, responses to the survey questions varied.

When asked about anticipated changes to improve board risk reporting, several executives cited the need for additional stress testing, further development and refining of key risk indicators, a shift of the board conversation to focus more on emerging and strategic

¹ *Board Risk Oversight – A Progress Report: Where Boards of Directors Currently Stand in Executing Their Risk Oversight Responsibilities*, Protiviti (commissioned by the Committee of Sponsoring Organizations of the Treadway Commission [COSO]), December 2010, available at www.protiviti.com.

² *Reporting Key Risk Information to the Board of Directors: Top Risk Executives Share Their Practices*, by Bruce Branson, Associate Director, North Carolina State University ERM Initiative, 2015, available at www.erm.ncsu.edu/library.

BOARD PERSPECTIVES: RISK OVERSIGHT

risks, renewed efforts to refine the risk appetite statement, and a more expanded look at risk velocity. The report discussed how much time was devoted to risk on the board agenda and, in some instances, how *little* time was devoted.

We agree there is no one-size-fits-all format to board risk reporting. It's a given that every organization is different from a strategic, operational, cultural and organizational standpoint; all of the above drive different reporting to the board. However, the state of play in board reporting raises the question as to whether a principled approach might give directors and executives more direction and clarity to their efforts to enhance board risk reporting.

Risk reporting should enable the board and its respective committees to understand and govern the organization's risks. To that end, we suggest six interrelated "board risk reporting principles" intended to foster reporting that focuses directors on the risks that matter and enables them to bring to bear their knowledge and expertise in ways that add and preserve enterprise value:

1. Focus the "lion's share" of risk reporting on the critical enterprise risks and emerging risks –

The critical enterprise risks represent the top risks that can threaten the company's strategy, business model or viability. These risks warrant the most attention from the board's risk oversight process. In addition, the board needs to be mindful of emerging risks triggered by unanticipated and potentially disruptive events of varying velocity, ranging from catastrophic events (e.g., a pandemic or hurricane) to existing risks accelerated by external and/or internal factors in unexpected ways (e.g., the impact of deterioration in underwriting standards, cheap money and demand for an endless supply of mortgage-backed securities on the sub-prime market leading up to the financial crisis).

Key Takeaway: These two categories of risk (including interrelated risks) provide a useful context for the full board and/or specific board committees to consider to ensure the scope of risk reporting is sufficiently comprehensive, forward-looking and focused on the risks warranting the most attention. Most likely, they relate to execution of the strategy and therefore potentially could be the most disruptive to the business model.

2. Address ongoing business management risks on an outlier basis and as an integral part of reporting on different areas of the business –

Every business has myriad operational, financial and compliance risks. If any of these risks are critical enterprise risks, they warrant the full board's attention with ongoing oversight by either the full board or a designated board committee. If not, risk reporting should focus on communicating these risk exposures to the board (or an appropriate committee of the board) through periodic status reports on line-of-business, product, geography, functional or program performance, as well as escalation of unusual matters requiring immediate board attention. For example, if there are exceptions against established limits (i.e., limit breaches) or a significant breakdown, error, incident, loss (or lost opportunity), close call or near miss in a critical area, it could warrant escalation to the board.

Key Takeaway: Reporting on the day-to-day risks should not be as frequent as the critical enterprise and emerging risks. The board does not have sufficient agenda time to consider every risk embedded within an organization's day-to-day operations. There has to be some prioritization.

3. Ensure risk reporting is linked to key business objectives –

Realistic and measurable objectives support the organization's overall strategy and business plan. Risks related to those objectives may impact the organization's ability to achieve them and execute the strategy and plan. The relevancy of risk reporting is more firmly established with directors when it is closely tied to business plans and the critical objectives and initiatives management has communicated to them. Some risks may affect multiple objectives, whereas others may require specific actions to address changing conditions to ensure achievement of objectives.

Key Takeaway: Risk reporting should be integrated with strategy, business objectives, business plans and performance management. Reporting is less effective when it is an afterthought to strategy and an appendage to performance management.

BOARD PERSPECTIVES: RISK OVERSIGHT

4. Use risk reporting to advance management’s risk appetite dialogue with the board – In the aforementioned Protiviti survey on board risk oversight,³ less than 15 percent of participating directors reported that discussions regarding acceptable levels of risk are sufficient for the board’s purposes. While we believe that the risk appetite dialogue has advanced at the board level over the past five years, there is still plenty of room for improvement. Once executive management and the board agree on the drivers of – and strategic, operational and financial parameters around – opportunity-seeking behavior, the resulting risk appetite statement is a reminder of the core risk strategy arising from the strategy-setting process. Risk reporting should disclose when conditions change and the agreed-upon parameters are approached or breached.

Key Takeaway: A winning strategy exploits to a significant extent the areas in which the organization excels relative to its competitors. The risk appetite statement serves as a guidepost when a new market opportunity or significant risk emerges. Risk reporting should call attention to the level of risk the organization is undertaking in the pursuit of creating value and achieving key objectives, and whether risk levels are consistent with risk appetite.

5. Integrate risk reporting with performance reporting – When stakeholders (e.g., owners of corporate, line-of-business, product, geography, functional or program performance goals) report on performance to the board, they should also disclose the related key risks. This linkage of opportunity and risks is important, as it enables each stakeholder reporting to the board to engage in a dialogue with directors on (a) the underlying risks and assumptions inherent in executing the strategy and achieving performance targets, (b) the “hard spots” and “soft spots” inherent in the performance plan, (c) the implications of

changes in the business environment on the core assumptions and desired risk levels underlying the strategy, and (d) the effectiveness of risk management capabilities.

Key Takeaway: The effectiveness with which risk reporting is integrated with performance reporting is a powerful indicator of the enterprise’s risk culture. If risk reporting is an appendage to performance reporting, risk is more likely to receive limited board agenda time. If risk reports disclose gaps in capabilities for managing priority risks, follow-up reporting is needed to ensure improvement initiatives are undertaken and kept on track.

6. Report on whether changes in the external environment are affecting critical assumptions underlying the strategy – Risk reporting should provide insights as to whether executive management’s assumptions about markets, customers, competition, technology, regulations, commodity prices and other external factors remain valid. Reporting should focus on whether changes in these environmental factors have occurred, which could alter the fundamentals underlying the business model.

Key Takeaway: Board risk reporting should focus on more than performance. It should use non-traditional information and data from both management and external sources that may offer directors a contrarian view. Boards place high value on “early warning” capability.

The above principles are not intended to prescribe specific reporting practices, but rather offer sound direction for the board and management to pursue. These principles are also focused on the substance and content of the reporting; therefore, such clichés as “keep it simple” and “use standard dashboards” are not included.

³ See *Board Risk Oversight – A Progress Report: Where Boards of Directors Currently Stand in Executing Their Risk Oversight Responsibilities*, available at www.protiviti.com.

BOARD PERSPECTIVES: RISK OVERSIGHT

Questions for Boards

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

- Does the board periodically evaluate the nature and frequency of management's risk reporting? Do directors work with management to agree on risk information the board and its committees require?
- Has the board considered the six principles outlined above in its ongoing efforts to focus and enhance the risk reporting it receives?
- Is the board satisfied that sufficient time is allocated to risk matters on the agendas of both the full board and various board committees? Do directors believe they receive sufficient information about changing risks to avoid the surprise factor?

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. We help organizations identify and prioritize the critical risks that can impair their reputation and brand image, and we assist with improving management's risk reporting to the board.

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.

Named one of the 2015 *Fortune* 100 Best Companies to Work For®, 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**.