

Board Perspectives: Risk Oversight

Five Risk Categories for Focusing Risk Oversight

Issue 16

As the board organizes itself for risk oversight, the question arises as to whether it should adopt its own risk language to ensure it is covering all bases. While each board must decide for itself whether a risk language is useful given the nature of the enterprise's operations, here we explore five risk categories directors may want to consider.

Key Considerations

We like the broad categories recommended by The National Association of Corporate Directors.¹ They apply to every company, regardless of its industry and strategy. Each is discussed below.

Governance risks. Periodically, boards of directors must consider CEO selection and compensation, board leadership and composition, board structure, and other governance issues critical to the enterprise's success. Often, these decisions require directors to weigh risks and rewards associated with alternative courses of action. While boards can benchmark their processes for evaluating these issues by considering relevant practices employed by other boards, they often must rely on their collective business judgment, knowledge of the business and information provided by third-party advisers, including search firms, compensation consultants and legal counsel.

Critical enterprise risks. Certain risks require directors to have the necessary information that will prepare them for discussions with management about the risks and how they are managed. Risks that threaten the company's strategy and the viability of its business model should command the board's risk oversight agenda. The criticality

Areas for Board Responsibility for Risk Oversight²

1. **Governance risks** – Risks related to directors' decisions regarding board leadership, composition and structure, director and CEO selection, and other governance matters.
2. **Critical enterprise risks** – The top five to 10 risks that can threaten the company's strategy, business model or viability.
3. **Board-approval risks** – The risks related to decisions the board must make with respect to important policy areas, such as major strategic initiatives, acquisitions or divestitures, major investments, entry into new markets, etc.
4. **Business management risks** – Risks associated with ongoing day-to-day business operations.
5. **Emerging risks** – External risks outside the scope of categories (1) through (4).

of these risks – such as credit risk in a financial institution or supply chain risk in a manufacturer – requires full board engagement, as well as an ongoing process to identify them. While management is responsible for addressing these risks, the board should consider its own information requirements for understanding them. For example, the board might require management to report on the impact and likelihood of the risk of key strategic goals as compared to other enterprise risks, as well as the status of risk mitigation efforts with input from the executives responsible for managing the risks. Other examples of ➤

¹Report of the NACD Blue Ribbon Commission – Risk Governance: Balancing Risk and Reward, National Association of Corporate Directors, October 2009, Appendix A, pages 22-23, <http://www.nacdonline.org/Store/ProductDetail.cfm?ItemNumber=675>.

²Ibid, page 9.

BOARD PERSPECTIVES: RISK OVERSIGHT

relevant information might include the effects of technological obsolescence, changes in the overall assessment of risk over time, the effect of changes in the environment on the core assumptions underlying the company's strategy, and interrelationships with other enterprise risks.

Board-approval risks. Through careful consideration and timely due diligence, directors must satisfy themselves that management's recommendations regarding strategic initiatives and other policy matters are appropriate to the enterprise before approving them. Therefore, such matters as proposed acquisitions, divestitures, major capital expenditures or new product lines may prompt the board to ask questions regarding the associated risks and rewards and even request further analysis before approving management's recommended actions.

Business management risks. Every business has myriad operational, financial and compliance risks embedded within its day-to-day operations. Because the board simply does not have sufficient time to consider every risk individually, it should identify specific categories of business risk that pose threats warranting attention and determine whether to oversee each category at the board level or delegate oversight responsibility to an appropriate committee. For example, the audit committee traditionally oversees financial reporting risks. Other business risks might include: operational risks associated with IT, intellectual property, customer fulfillment, product obsolescence, and environmental and safety issues; financial risks, such as excessive leveraging of the balance sheet; compliance risks, including noncompliance with a new complex law; and reputational risks, such as those that threaten the company's brand image. With respect

to all of these risks, it is management's responsibility to address them. If any are critical enterprise risks, they warrant the full board's attention (as noted earlier).

Emerging risks. Management is responsible for addressing those external environment risks outside of the scope of the risks noted above; however, directors may need to understand them. The effects of demographic shifts, climate change, catastrophic events and new security threats are examples. Directors need to know that effective processes are in place to update the company's risk assessment as the environment changes.

The above risk categories provide a useful context for boards to consider to ensure the scope of the risk oversight process is sufficiently comprehensive.

Questions for Directors

Following are some suggested questions that boards of directors may consider in the context of the nature of the entity's risks inherent in its operations:

- Is there a process for identifying the organization's critical enterprise risks for purposes of prioritizing the board's risk oversight focus with management?
- Is the board approving major strategic and policy issues on a before-the-fact basis?
- Is there a process in place for identifying and communicating emerging risks to enable management and the board to be proactive?

How Protiviti Can Help

Protiviti provides an experienced unbiased perspective in assisting directors with understanding their organizations' key risks and how they are managed.

About Protiviti

Protiviti (www.protiviti.com) is a global business consulting and internal audit firm composed of experts specializing in risk, advisory and transaction services. The firm helps solve problems in finance and transactions, operations, technology, litigation, governance, risk, and compliance. Protiviti's highly trained, results-oriented professionals provide a unique perspective on a wide range of critical business issues for clients in the Americas, Asia-Pacific, Europe and the Middle East.

Protiviti has more than 60 locations worldwide and is a wholly owned subsidiary of Robert Half International Inc. (NYSE symbol: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.