Board Perspectives: Risk Oversight

Five Risk Oversight Questions Directors Should Ask

Issue 50

There are many questions directors can ask about the organization's risks and risk management as they discharge their risk oversight responsibilities. As the business environment changes, risk profiles change and business models are exposed to disruption. Corporate strategies and risk management capabilities must keep pace in response to these changes.

Key Considerations

In this dynamic environment, we offer five questions for boards to consider as they take a fresh look at their risk oversight agenda for 2014:

1. **Does our risk profile reflect the significant risks we face currently?** When management reports on the company's top risks, the reporting should highlight (a) whether the noted risks increased or decreased, (b) any risks that are new, and (c) whether the current summary excludes risks previously reported. In addition to addressing severity of impact and likelihood of occurrence, it may be useful to prioritize "high impact, low likelihood" risks in terms of their reputational effect, velocity to impact, and persistence of impact, as well as the enterprise's response readiness. Such insights can pinpoint areas where the company may need response plans for unlikely extreme events. As risk assessments can go stale rather quickly, the company should strive to keep them fresh.

   A critical aspect of keeping a risk profile current is the timely identification of emerging risks. There are a variety of ways to identify these risks. For example: (1) focus on whether critical assumptions underlying the strategy are becoming, or have become, invalid; (2) pay attention to global trends that have relevant strategic underpinnings; (3) evaluate the effects of the organization's pre-emptive actions to reach beyond its core business (e.g., acquire a completely different line of business); (4) apply scenario analysis to the business plan, ensuring the worst-case scenario is extreme enough; and (5) consider relevant "game changing" risks (e.g., cybersecurity threats, significant demographic changes, infrastructure fragility, fiscally distressed cities, and any other critical risks germane to the organization's business model).

2. **Are we improving our risk management capabilities continuously to ensure we are managing our risks effectively in a changing business environment?** Once the key risks are targeted, someone or some group, function or unit must own them. Gaps and overlaps in risk ownership should be minimized, if not eliminated, so accountability for results is firmly established with the lines of business and process owners. The effectiveness of the board's oversight of this ongoing continuous improvement of risk management capabilities is directly impacted by its ability to obtain substantive risk information from internal sources and, when appropriate, outside

sources. To that end, the board should satisfy itself that (1) a robust process for managing and monitoring each of the critical enterprise risks is in place, including effective response plans in the event of a crisis; (2) risk management capabilities are improved continuously as the speed and complexity of business changes; and (3) reporting on risks and risk management performance is timely and reliable. There may be opportunities to enhance the risk reporting process to make it more effective and efficient, and the board should consider them in light of its needs.

3. **Are the board and executive management on the same page with respect to appetite for risk?** The board should engage management in a periodic dialogue about the risks the enterprise should take, the risks it should avoid and the parameters within which it should operate. A robust risk appetite dialogue frames the following question: "How do we know we are executing our business model within the parameters of our risk appetite?" The only way to know for sure is to decompose the risk appetite statement into more specific risk tolerances and use them to manage performance variability around the achievement of business objectives. For example, separate risk tolerances may be expressed for objectives relating to earnings variability, interest rate exposure, and the acquisition, development and retention of people.

4. **Is our risk culture encouraging the right behaviors?** Even the most well-intentioned risk management process can be compromised if dysfunctional organizational behavior exists and is allowed to fester. If the chief executive officer (CEO) chooses to ignore the warning signs posted by the risk management function, the reward system is focused primarily on short-term performance targets, the board is not asking the tough questions about the assumptions and risks underlying the strategy, and risk management is not positioned effectively within the organization, it is not likely risk management's voice will be heard at the crucial moment. If there is a lack of transparency in a highly complex organizational structure, tolerance for conflicts of interest and self-dealing, a shoot-the-messenger or warrior culture and other dysfunctional behaviors, the organization is likely to miss market-driven changes in critical assumptions underlying the strategy. This can lead to inappropriate risk-taking or even failure to exit a flawed strategy in a timely manner. A risk culture conducive to effective risk management reflects the shared values, goals, practices, reinforcement mechanisms and attitudes that embed risk into an organization's decision-making processes and risk management into its operations. An effective risk culture encourages open communication, sharing of knowledge and best practices, continuous process improvement, and a strong commitment to ethical and responsible business behavior. More important, it appropriately balances entrepreneurial activities and control activities so that neither is too disproportionately strong relative to the other, meaning a healthy tension exists between the two.

5. **Have we integrated risk management with the appropriate management processes?** The relevance of risk management increases if it is integrated with core management processes. The idea is to integrate risk management with what matters to instill in the board, CEO and executive management greater confidence that the organization will be successful in achieving its objectives and executing its strategy. The nature and extent of integration vary from industry to industry and company to company, and are highly dependent on management's operating style. The scope of integration could include such processes as strategy-setting, annual business planning, performance management, budgeting, competitive intelligence, capital expenditure funding, and merger and acquisition (M&A) targeting, due diligence and integration. Effective integration can result in the risk management process becoming more aligned with the rhythm of how the business is run and managed so that it can make value-added contributions to establishing sustainable competitive advantage and improving business performance.

The above questions can provide a framework for taking a fresh look at the board's risk oversight agenda given changes in the business environment. Answers to these questions may provide insight on how the company can improve its risk management capabilities.

Questions for Boards

The board of directors may want to consider the above questions in the context of the nature of the entity's risks inherent in its operations.

How Protiviti Can Help

As the board continues to refine and improve its risk oversight process, Protiviti can assist it and executive management with identifying and assessing the enterprise's risks and implementing strategies and tactics for managing risk. We assist companies with integrating their risk assessment process with their core business processes, including strategy-setting. We also help organizations improve their risk reporting to better inform the board's risk oversight process.

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. Through our network of more than 70 offices in over 20 countries, we have served more than 35 percent of FORTUNE 1000® and FORTUNE Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

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.directorship.com/author/jim-deloach/ in the "Blogs & Opinion" section. A compilation of blog posts and articles is maintained and categorized by author's name. Twice per year, the six most recent issues of *Board Perspectives: Risk Oversight* will be consolidated into a printed booklet that will be co-branded with NACD. Protiviti will also post these articles at Protiviti.com.

protiviti®
Risk & Business Consulting.
Internal Audit.