Board Perspectives: Risk Oversight

Should the Board Have a Separate Risk Committee?

Issue 72

A separate risk committee of the board of directors is not a panacea, nor is it a one-size-fits-all solution. What are the circumstances in which it may be appropriate to have one, what value does it contribute to the board's overall risk oversight responsibilities, and how should it be organized? We explore these and other related topics below.

Risk oversight is the process applied by the board of directors to determine that the company has a process in place for managing its significant risks and is improving that process continuously as the business environment changes. While there are alternative models for organizing risk oversight, the full board retains overall responsibility for the risk oversight process, in effect, mirroring its overall responsibility for oversight of strategy and policy.

Key Considerations

In one approach to risk oversight, the full board coordinates risk oversight scope and accountabilities. The board's risk oversight responsibilities are assigned to its various standing committees, with such responsibilities addressing, at minimum, the risks inherent in the scope of each committee's activities as set forth in its respective charter. The full board receives reports from each committee and from management regarding the status of critical risks and recommendations for risk-related considerations to place on the full board's agenda.

In another approach, the board may delegate its overall responsibility to a designated committee. For many boards, the audit committee may be the default committee to receive this assignment, because the New York Stock Exchange listing standards require that the audit committee charter for listed companies include the committee's duties and responsibilities to discuss risk assessment and risk management policies. For that reason, the audit committee often has the most involvement in the board's risk oversight process, either overall or related to specific risks germane to its prescribed activities.

In lieu of the audit committee, the full board may delegate its overall responsibility to a designated risk committee (i.e., a board committee, not a management committee) to oversee risks specifically included within the scope of its charter. These risks vary widely based on the nature of the industry and the complexity of the organization's risk profile, requiring focused expertise to provide appropriate oversight. Among other things, a designated risk committee might oversee the company's risk management framework, oversee management's determination of critical risks and risk management capabilities, and periodically report risk oversight findings to the full board.

Perhaps the most compelling reason for a separate risk committee is the complexity of the business environment, as evidenced by the nature of the industry and business model, the risks inherent in the organization's strategy and the sophistication of the risk management

infrastructure. Equally as compelling, the collective agendas of the full board and the various standing committees may be too packed to give risk oversight sufficient attention, and the audit committee may be too focused on financial reporting matters or lack the requisite expertise to provide the default solution noted above.

There may be important benefits to consider when evaluating the merits of a separate risk committee. An enterprisewide approach to risk oversight, an opportunity to obtain and focus risk management experience, more effective anticipation of and reaction to events and trends that could lead to disruptive change, and a stronger focus on specific critical enterprise risks – such as technology, litigation and environmental issues – are all examples. Extenuating circumstances may warrant consideration – for instance, a history of surprises, significant work required to improve risk management capabilities and/or a need to strengthen risk culture. Worse, there may be a lack of confidence in management.

Whatever the business case supporting a separate risk committee, there may be arguments against it. For example, risk oversight is an overall board responsibility that must be embedded in – and not segregated from – board discussions regarding strategy, policy, execution and reporting. Various board committees naturally address risk through their respective chartered activities. Therefore, a separate risk committee might contribute to confusion over where the responsibilities of one committee end and others begin, leading to possible gaps and overlaps. Another consideration is that the board cannot be certain in advance whether a risk committee will accomplish its intended objectives.

The above discussion indicates that there are many factors to take into account when evaluating whether a separate risk committee is appropriate. Once a decision is made to form a separate risk committee, the board must decide the committee's role. Given that there is no one-size-fits-all standard, each board must make this determination based on the facts and circumstances in each case. With this in mind, the following are some suggested responsibility areas to consider when defining the risk committee's charter:

- **Ensure risk is appropriately considered in strategy-setting and business planning –** Evaluate whether appropriate risks are taken in the pursuit of value creation, and challenge management's assumptions underlying key decisions and strategies. Provide input to management regarding the enterprise's risk appetite and risk tolerances and limit structures, both overall and by line of business.
- **Oversee monitoring of the organization's risk profile –** Ascertain whether management is identifying, assessing and monitoring the types, levels and concentrations of risk, both by line of business and enterprisewide. Ensure that the risk profile remains within the company's risk appetite and that there is a process for identifying emerging risks. Discuss the critical enterprise risks and emerging risks with management, and understand the response strategies for addressing them.
- **Oversee the risk management organization –** Approve companywide policies with respect to risk assessment and risk management practices. If there is a management risk committee, approve its charter to ensure that the committee's activities are in accordance with expectations and are adequately informing the board. If there is a chief risk officer (CRO) or equivalent executive, review his/her appointment, performance and replacement in consultation with the full board; ensure he/she has sufficient stature, authority and independence within the organization; and oversee his/her activities through ongoing communications and risk reporting and periodic executive sessions.
- **Oversee management's implementation of risk responses –** Understand and approve the organization's risk management infrastructure and program, and oversee whether the critical risks are being monitored and managed effectively within established risk tolerances and limits. Review crisis management plans to ensure management has actionable response plans in place to address potentially disruptive risks, including extreme black swan events. Understand, provide input to and approve the risk reports the committee receives from management in discharging the scope of its risk oversight responsibilities.
- **Influence risk culture –** Promote an open and positive risk culture such that personnel at all levels

of the organization manage risks rather than take them recklessly or avoid them altogether. Oversee communications about escalating risks on a timely basis, and pay attention to the warning signs of a dysfunctional culture. Oversee remediation of issues (e.g., limits violations, near misses, policy non-compliance, control deficiencies) to ensure they are addressed in a timely manner.

- **Report to and advise the full board, and coordinate risk oversight with other board committees –** Advise the board on risk strategy, and ensure that the board's risk oversight is focused on the critical enterprise risks and emerging risks (i.e., the risks that matter). Annually present to the full board a report summarizing the committee's review of the company's risk management program, including deficiencies noted. Recognize the responsibilities delegated to other board committees, and meet and coordinate with these committees to avoid gaps and overlaps in the board's overall risk oversight process. Coordinate with the audit committee to understand how the organization's internal audit plan is aligned with its key risks. Establish criteria for risk reporting to the board, and recommend the same for board approval. Review the charter at least annually; update it as needed to respond to changing risk profiles, oversight priorities, and regulatory or other requirements; and submit the charter to the full board for approval. Review risk- and board risk oversight-related disclosures in public reports, and provide input to the board and audit committee.
- **Consult external experts as necessary –** Obtain expert advice regarding risk-related matters. When conducting investigations into any matters within the committee's scope of responsibility, obtain advice and assistance from outside advisers as necessary.

The above summary is illustrative and is intended to be neither exhaustive nor prescriptive. The board dictates the scope of the risk committee, delegating responsibilities consistent with the board's overall charter and the corporate bylaws.

Once the board decides what the risk committee is to accomplish, determining the committee's composition, selecting the appropriate members and setting meeting frequency and agendas must be addressed. With respect to composition and the selection process, there are several factors to evaluate:

- Consider whether membership of the committee should be limited to or consist primarily of independent directors.
- Determine the experience and skills necessary for an effective risk committee member. Hopefully, some directors currently serving on the board will meet these requirements. If not, when searching for director candidates to serve on the committee, make sure they have the right "fit" in terms of personality, team orientation, leadership and communication skills, enabling them to work with other committee members, the board and management. In addition, consider how the organization can attract, cultivate and retain appropriate committee members (e.g., succession planning and appropriate continuing education).
- Consider whether a "risk expert" should serve on the committee (i.e., someone with a background in risk management or oversight relevant to the nature of the organization's operations). This role is analogous to the financial expert serving on the audit committee.
- In defining the terms of service for members and the committee chair, note that term limits may not be desirable because of the need for continuity and the limited pool of candidates. In selecting the committee chair position, note that the chair may be rotated, appointed or reappointed by the board chair; elected by majority committee vote; or selected by other means.

Regarding meeting frequency, consider the nature and volatility of the organization's strategy, operations and risks. Also, consider the scope of responsibilities outlined in the committee charter, which often sets forth the expected meeting frequency (e.g., meet at least quarterly, or more frequently as necessary). The more granular the charter, the easier it is to lay out an annual calendar.

Meeting agendas might include specific risk issues (e.g., drill-downs on specific risks and risk responses or evaluation of risk appetite) and other activities (e.g., risk committee education). Agendas should be developed

based on suggestions from committee members and approved by the committee chair. The risk committee calendar should be coordinated with the respective calendars of the audit, compensation and other committees to coordinate activities and resources. Briefing materials should be provided in advance of each regularly scheduled meeting, which should begin or conclude with an executive session. The committee should meet periodically with executive management, line of business leaders, the CRO (or equivalent executive) and the chief audit executive. At least annually, the chair should ascertain that the committee's activities fulfill the expectations set forth within the charter.

Questions for Boards

The following are some suggested questions that boards may consider, based on the risks inherent in the entity's operations.

If there is a separate risk committee of the board:

- Does the committee have access to the company executives, resources and information it needs to carry out its oversight responsibilities? Does it include a risk expert?
- How will the board ensure that the committee chair, the committee itself and its individual members are evaluated?
- Is the committee adequately funded? Does it have access to outside experts? Have risk oversight responsibilities been delineated (i.e., which risks will the risk committee oversee, and which risks will be left to other board committees to oversee)?
- If there is a CRO (or equivalent executive) and/or a management risk committee, does the committee have sufficient transparency into their activities?
- Is the committee fulfilling its chartered responsibilities?

How Protiviti Can Help

Protiviti assists directors in public and private companies with their oversight of the processes for identifying and managing the organization's key risks. We provide an experienced, unbiased perspective on issues separate from those of company insiders and an analytical assessment approach that is aligned with the unique characteristics of the risks the company faces.

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* 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.