INSIGHTS
The Corporate & Securities Law Advisor

VOLUME 30, NUMBER 9, SEPTEMBER 2016

CORPORATE GOVERNANCE

Risky Business: Is It Time to Consider Establishing a Separate Risk Committee?

Corporate boards increasingly are considering whether it is in the best interests of the board, the company and its shareholders to establish a separate risk committee. Investors, proxy advisory firms and other corporate governance advocates also have developed expectations with respect to board risk oversight responsibilities.

By William M. Libit and Todd E. Freier

Oversight of a company's enterprise risks recently has evolved into one of the board's most critical fiduciary duties and responsibilities. Since enterprise risks do not remain static and are often interrelated and complex, it is imperative that boards maintain continuous risk oversight. Risks relating to cybersecurity, regulations and corporate reputation, for example, now, more than ever, necessitate effective board oversight.[1] A 2016 study revealed that nearly 60 percent of surveyed companies believe they are facing a greater volume and complexity of risks than they were five years ago and less than half have boards that "extensively" or "mostly" include top risk exposures when discussing the company's strategic plan.[2] In response to this evolving and complex risk environment, corporate boards increasingly are considering whether it is in the best interests of the board, the company and its shareholders to establish a separate risk committee.

William M. Libit *is a partner, and* **Todd E. Freier** *is senior counsel, at Chapman and Cutler LLP in Chicago, IL.*

Risk Oversight and Corporate Governance

Background

Current legal and regulatory frameworks impose a board's general duty to provide risk oversight and disclosure relating thereto.[3] Former SEC Commissioner Aguilar recently commented that a robust corporate governance framework is exemplified by effective risk oversight.[4] Common practice among U.S. public company boards is to delegate the majority of this oversight duty to their audit committees, with oversight of certain specific risks to other standing board committees (*e.g.*, compensation risk oversight being the responsibility of the compensation committee). The full board, however, is ultimately responsible for a company's risk oversight.

Although still uncommon outside of the financial services sector, some boards are addressing both the importance of providing robust risk oversight and the heavy workload of their audit committees by establishing separate risk committees to which

audit committees (and other board committees, as the case may be) delegate certain of their enterprise risk oversight responsibilities.[5] In addition to certain financial institutions being required by the Dodd-Frank Act to have a separate risk committee, various institutional investors and corporate governance advocates, as further discussed below, are also encouraging boards to establish a separate risk committee.[6]

A robust corporate governance framework is exemplified by effective risk oversight.

Arguments For and Against

Arguments for and against creating a separate board risk committee include the following:

For	Against
■ enterprise risks are too numerous and complex and require a separate board committee to provide adequate oversight ■ allows a board committee to focus solely on enterprise risks and, if necessary, coordinate risk oversight with other board committees ■ provides greater support to officers who are responsible for risk management processes ■ facilitates a continuous review of enterprise risks ■ focuses the board on nominating directors with risk expertise ■ many audit committees no longer have the time, expertise or resources necessary to provide oversight of all enterprise risks ■ demonstrates to shareholders and other stakeholders that the board is committed to overseeing risks ■ is viewed by certain institutional investors and corporate governance advocates as an emerging best practice[7]	■ is unnecessary, as current board committees (*e.g.*, audit, compensation and governance) already provide sufficient/expert risk oversight ■ another standing board committee will consume valuable board resources, increase organizational costs and dilute the board's focus ■ certain industry-specific enterprise risks are so significant and complex that they require separate board oversight committees (*e.g.*, IT committee, environmental committee, health and safety committee, finance committee) ■ creates risk oversight inefficiencies and confusion (*e.g.*, potentially duplicating committee oversight responsibilities) ■ certain risks (*e.g.*, relating to cybersecurity and corporate strategy) are more appropriately overseen by the entire board, not just a committee

Positions of Institutional Investors, a Proxy Advisory Firm and Corporate Governance Advocates

There is no one-size-fits-all approach to corporate governance and enterprise risk oversight. The unique characteristics of the company, the complexity of the industry in which it operates (e.g., with respect to regulatory, financial, credit and commodity risks), the needs of company stakeholders and the adoption of corporate governance policies the company and its board feel are essential in generating long-term shareholder value often dictate, in part, whether a board establishes a separate risk committee or delegates risk oversight duties and responsibilities among existing board committees. As boards evaluate whether to establish a separate risk committee, it may be helpful to understand the current risk oversight policies and positions of several large institutional investors, a leading proxy advisory firm and certain corporate governance advocates, as this understanding provides insight into the general expectations of these parties with respect to corresponding duties and responsibilities. A select summary of those policies and positions is provided below.

Institutional Investors—Asset Managers

- ***BlackRock, Inc.***
  - — encourages companies to provide transparency as to the optimal risk levels, how risk

is measured and how risks are reported to the board and is particularly interested to understand how risk oversight processes evolve in response to changes in corporate strategy and/or shifts in the business and related risk environment
  - — believes that boards should clearly explain their approach to risk oversight, including where accountability lies within the boardroom for this activity, especially where there are multiple individuals or board committees tasked with oversight of various risks
  - — expects companies to identify and report on the material, business-specific social, ethical and environmental risks and opportunities and to explain how these are managed[8]
- ***State Street Global Advisors***
  - — believes that good corporate governance necessitates the existence of effective risk management systems, which should be governed by the board, and that directors have to monitor the risks that arise from a company's business, including risks related to sustainability issues
  - — encourages companies to be transparent about the environmental and social risks and opportunities they face and to adopt robust policies and processes to manage such issues[9]
- ***Allianz Global Investors*** strongly supports the establishment of a separate and independent risk committee responsible for supervision of risks within the company; if necessary, the risk committee should seek independent external support to supplement internal resources[10]

Institutional Investors—Pension Funds

- ***California Public Employees' Retirement System*** recommends, among other things, that the board (1) be comprised of directors with a balance of broad business experience and extensive industry expertise to understand and question the breadth of risks faced by the company (as the board is responsible for a company's risk management philosophy, organizational risk framework and oversight), (2) consider risk management a priority and devote sufficient time to risk oversight, (3) set out specific risk tolerances and implement a process that continuously evaluates and prioritizes both internal company-related and external risks, (4) at least annually, approve a documented risk management plan and disclose sufficient information to enable shareholders to assess whether the board is carrying out its risk oversight responsibilities, (5) establish a risk committee (be it a standalone or combined committee), which can be an effective mechanism to provide transparency, focus and independent judgment to oversee the company's risk management approach, and (6) assign executive management with designing, implementing and maintaining an effective risk program even though the board is ultimately responsible for risk oversight[11]
- ***California State Teachers' Retirement System***
  - — asserts that the board should disclose its risk oversight process and responsibilities to ensure that the company is effectively managing, evaluating and mitigating its risk profile and risk management plan
  - — mentions that the board should regularly review and approve the risk management plan that management will implement[12]
- ***Florida State Board of Administration***
  - — generally encourages companies, especially financial companies, to have a standing enterprise risk management committee with formal risk management oversight responsibilities
  - — may withhold support for individual directors if there are indications that certain directors failed to understand company risk exposures and/or failed to take reasonable steps to mitigate the effects of the risk, leading to large losses[13]

Proxy Advisory Firm

- ***Glass, Lewis & Co., LLC***
  - — evaluates the risk management function of a board on a strictly case-by-case basis
  - — believes that financial firms should have a chief risk officer reporting directly to the board and a dedicated risk committee or a committee of the board charged with risk oversight, and that non-financial firms which maintain strategies that involve a high level of exposure to financial risk (e.g., complex hedging or trading strategies) should also have a chief risk officer and a risk committee
  - — recommends that shareholders vote "against" committee members where it is found that the company's board-level risk committee's poor oversight contributed to any significant losses or write-downs on financial assets and/or structured transactions
  - — considers recommending that shareholders vote "against" the chair of the board in cases where a company maintains a significant level of financial risk exposure but fails to disclose any explicit form of board-level risk oversight (committee or otherwise)
  - — recommends that shareholders vote "against" directors responsible for risk oversight in cases where the board or management has failed to sufficiently identify and manage a material environmental or social risk that did or could negatively impact shareholder value[14]

Corporate Governance Advocates

- ***Council of Institutional Investors*** (advocating on behalf of shareholders)
  - — asserts that the board has ultimate responsibility for risk oversight and should (1) establish a company's risk management philosophy and risk appetite, (2) understand and ensure risk management practices for the company, (3) regularly review risks in relation to the risk appetite, (4) evaluate how management responds to the most significant risks and (5) disclose to shareholders, at least annually, sufficient information to enable them to assess whether the board is carrying out its oversight responsibilities effectively
  - — believes that effective risk oversight requires regular, meaningful communication between the board and management, among board members and committees, and between the board and any outside advisers it consults, about the company's material risks and risk management processes[15]
- ***The Business Roundtable*** (advocating on behalf of management)
  - — expects the board to oversee the significant risks facing the company and the processes that management has implemented to identify and manage risk
  - — notes that unless the full board or another committee does so, the audit committee should oversee the company's risk assessment and risk management process; however, the audit committee should not be the sole body responsible for risk oversight and the board may decide that it is appropriate to allocate responsibility for some types of risk to other committees or to the board as a whole
  - — states that no one risk oversight structure is right for every board, and different structures may be appropriate depending on a company's industry and other factors; nevertheless, the board should understand the structure it has put in place and be satisfied that it provides the board with the information it needs to understand all of the company's major risks and the way in which they interact with the company's strategy and are being addressed
  - — maintains that committees with risk-related responsibilities should report regularly to

the full board on the risks that they oversee and brief the audit committee, as appropriate, in cases where securities market listing standards require the audit committee to retain some risk oversight responsibility (e.g., NYSE)[16]

Considerations for Boards of Directors

To facilitate discussion among board members as to whether establishing a separate risk committee will contribute to more effective corporate governance and is in the best interests of the company, directors may consider the following.

Evaluate Current Risk Management and Oversight Processes

Given the evolving and complex risk environment currently confronting companies, it is essential that boards make enterprise risk oversight a priority. In a 2015 survey, 65 percent of surveyed directors indicated that they want their boards to spend at least "some" or "much more" time and focus on IT risks (including cybersecurity), while 47 percent indicated the same with respect to risk management generally.[17] To determine whether a separate risk committee will contribute to more effective corporate governance and is in the best interests of the company, a board should conduct a comprehensive evaluation of its current risk management and oversight processes, including, for example, (1) evaluating the board's and company's current risk assessment, oversight, mitigation and reporting processes, (2) defining and clearly understanding the risk appetite of the company, (3) reviewing existing committee charters for risk oversight responsibilities, (4) assessing the adequacy of the risk-related public disclosures made by the company (*e.g.*, in the "Management's Discussion and Analysis of Financial Condition and Results of Operations" and "Compensation Discussion and Analysis" sections of various SEC filings) and (5) monitoring the risk-related expertise of current board members to determine if additional expertise (whether general risk management or specific key risks relating to, for example, finance, cybersecurity or the environment) is necessary for the board to fulfill its oversight obligations.

Request Additional Risk-Related Information

The board's ability to implement effective corporate governance depends, in part, on the information the board receives from management. A risk committee (whether separate or combined with another committee) cannot necessarily identify and address lapses in a company's risk management processes without receiving relevant information and insights from management and other external sources. Notably, 69 percent of directors "somewhat" or "very much" wish that their boardroom materials better highlighted risks related to the particular issue being discussed.[18] Further, research reveals that there exists a certain disconnect as to what risks directors and management identify as most significant to their company. For example, directors tend to focus on risks associated with economic conditions, succession/human capital and political conditions, to name a few, while management tends to focus on risks relating to, among others, regulatory changes, cyber threats, customer loyalty and competitors.[19] Therefore, directors may not be receiving the pertinent risk-related information and materials they need to (1) fulfill their risk oversight obligations, generally, and (2) assess whether establishing a separate risk committee is in the long-term best interests of the board, company and shareholders, specifically.

Draft a Risk Committee Charter

Prior to establishing a separate risk committee, the board should draft a charter for a prospective risk committee. Such a charter, similar to other standing committee charters, should address the committee's purpose/objectives, committee composition (*e.g.*, size and member qualifications), committee leadership and meeting structures, committee self-evaluation procedures and, most important, delineate the duties and responsibilities of committee members. This

exercise will assist a board with carefully considering how it intends to define and implement risk oversight duties and responsibilities and thereby help in evaluating whether such a committee is consistent with and a necessary element of the board's and company's corporate governance strategies. If a separate risk committee ultimately is determined to be in the best long-term interests of the board, the company and its shareholders, it will be necessary to review the charters of other committees to ensure that they align with the new risk committee charter.

Benchmark Peer Board Committee Structure

Companies regularly should benchmark their enterprise risk oversight processes and board committee structure with those of their peers and the industry in which they operate (as an outlier may become the target of activist shareholder campaigns or be identified by institutional investors as an organization with potentially problematic risk oversight and governance practices). If a majority of peer companies have a separate risk committee and your board does not, the board should analyze the reasons behind this and determine whether such a committee might be in the best interests of the board, the company and its shareholders.

Ensure Substance over Form

Regardless of whether or not a board decides to establish a separate risk committee, it is imperative that the board adequately address its enterprise risk oversight duties and responsibilities and ensure that the substance of such duties and responsibilities trump the form (*e.g.*, by way of a separate committee or multiple board committees) in which they are identified, implemented and executed.

Notes

1. *See Risk Sensing: The (Evolving) State of the Art*, Deloitte (2015) (providing survey results of certain executives representing major industries, which revealed the three risk areas having the greatest impact on their companies' business strategy:

In 2013	*In 2015*	*Predicted for 2018*
1. reputation	1. regulatory	1. pace of innovation/ regulatory (tie)
2. business model	2. reputation	2. talent
3. economic trends/ competition (tie)	3. pace of innovation	3. reputation).

See also *Conduct Risk Report 2015/2016*, Thomson Reuters (2016) (revealing that conduct risk, which focuses on the corporate culture and ethical behavior of employees and managers, is receiving significant board attention, as 52 percent of surveyed global financial services firms reported an increase in board-level focus on this risk over the past 12 months and 63 percent expect the cost of time and resources devoted to conduct risk issues to increase in the next year).

2. *2016 The State of Risk Oversight: An Overview on Enterprise Risk Management Practices*, Mark Beasley, Bruce Branson and Bonnie Hancock (April 2016).
3. See, for example, Securities and Exchange Commission (SEC) Regulation S-K, Item 407(h), mandating that reporting companies, in certain periodic reports, disclose the extent of the board's role in the risk oversight of the company, such as how the board administers its oversight function and the effect this has on the board's leadership structure. In addition, *see* the listing requirement set forth in New York Stock Exchange (NYSE) Section 303A.07(b)(iii)(D), requiring every audit committee to have a written charter that addresses its duties and responsibilities which, at a minimum, must include (among other items) a discussion of policies with respect to risk assessment and risk management. Commentary to this listing requirement states:

> While it is the job of the CEO and senior management to assess and manage the listed company's exposure to risk, the audit committee must discuss guidelines and policies to govern the process by which this is handled. The audit committee should discuss the listed company's major financial risk exposures and the steps management has taken to monitor and control such exposures. The audit committee is not required to be the sole body responsible for risk assessment and management, but, as

stated above, the committee must discuss guidelines and policies to govern the process by which risk assessment and management is undertaken. Many companies, particularly financial companies, manage and assess their risk through mechanisms other than the audit committee. The processes these companies have in place should be reviewed in a general manner by the audit committee, but they need not be replaced by the audit committee.

4. *The Important Work of Boards of Directors*, 12th Annual Boardroom Summit and Peer Exchange, SEC Commissioner Luis A. Aguilar (October 14, 2015).
5. In 2015, 12 percent of S&P 500 company boards had a separate risk committee (up from 9 percent in 2014 and 4 percent in 2010). *2015 Spencer Stuart Board Index*, Spencer Stuart (November 2015). This increase may also be attributed, in part, to Section 165(h) of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank Act), which requires certain financial institutions to have such committee. Financial sector companies comprise approximately 18 percent of the S&P 500 index. *S&P 500 Financials*, S&P Dow Jones Indices, McGraw Hill Financial (February 29, 2016). *See* footnote 6 below for further discussion regarding Section 165(h) of the Dodd-Frank Act.
6. The Dodd-Frank Act requires a separate risk committee for (i) nonbank financial companies supervised by the Board of Governors of the Federal Reserve System that are publicly traded companies and (ii) certain bank holding companies that are publicly traded and have total consolidated assets of not less than $10 billion. The Board of Governors may require a publicly traded company with total consolidated assets of less than $10 billion to establish a risk committee to promote sound risk management practices. Under the Dodd-Frank Act, a risk committee shall (a) be responsible for the oversight of the enterprise-wide risk management practices of the nonbank financial company supervised by the Board of Governors or bank holding company, (b) include such number of independent directors as the Board of Governors may determine appropriate, based on the nature of operations, size of assets and other appropriate criteria related to the nonbank financial company supervised by the Board of Governors or a bank holding company and (c) include at least one risk management expert having experience in identifying, assessing and managing risk exposures of large, complex firms. Dodd-Frank Act, Section 165(h).
7. *See* discussion under "Current Policies and Positions of Certain Institutional Investors, a Proxy Advisory Firm and Corporate Governance Advocates as They Relate to Risk Oversight" herein. Further, note that certain activist investors are submitting shareholder proposals on this issue. For example, in 2015, the Construction Laborers Pension Trust Fund for Southern California submitted a shareholder proposal to Chesapeake Energy Corporation requesting that Chesapeake establish a risk oversight committee of the board, arguing, in part, that the SEC supports such proposal ("[The SEC notes] that there is widespread recognition that the board's role in the oversight of a company's management of risk is a significant policy matter regarding the governance of the corporation. In light of this recognition, a [shareholder] proposal that focuses on the board's role in the oversight of a company's management of risk may transcend the day-to-day business matters of a company and raise policy issues so significant that it would be appropriate for a shareholder vote."). Division of Corporation Finance, SEC, Staff Legal Bulletin No. 14E (October 27, 2009). Said proposal received 3 percent shareholder support (based on votes "for" and "against") at Chesapeake's May 22, 2015 annual meeting of shareholders.
8. *Proxy Voting Guidelines for U.S. Securities*, BlackRock, Inc. (February 2015).
9. *Proxy Voting and Engagement Guidelines – United States*, State Street Global Advisors (March 2016).
10. *Corporate Governance Guidelines and Proxy Voting Policy*, Allianz Global Investors (August 2015).
11. *Global Governance Principles*, California Public Employees' Retirement System (March 14, 2016).
12. *Corporate Governance Principles*, California State Teachers' Retirement System (April 3, 2015).
13. *2016 Corporate Governance Principles & Proxy Voting Guidelines*, Florida State Board of Administration (2016).
14. *Proxy Paper Guidelines 2016 Proxy Season: An Overview of the Glass Lewis Approach to Proxy Advice (United States)*, Glass, Lewis & Co., LLC (November 2015). Notably, our

research revealed that Institutional Shareholder Services Inc., another leading proxy advisory firm, does not publicly disclose a formal position that specifically addresses the establishment of a standing risk committee.

15. *Corporate Governance Policies*, Council of Institutional Investors (April 1, 2015).
16. Letter to the SEC in response to the SEC's Concept Release on Possible Revisions to Audit Committee Disclosures, The Business Roundtable (September 8, 2015).
17. *Governing for the Long Term: Looking Down the Road with an Eye on the Rear-View Mirror, PwC's 2015 Annual Corporate Directors Survey*, PricewaterhouseCoopers LLP (2015).
18. *Id*.
19. *Executive Perspectives on Top Risks for 2016: Key Issues Being Discussed in the Boardroom and C-Suite*, North Carolina State University's Enterprise Risk Management Initiative and Protiviti (March 2016).