



Corporate Responsibility Alert

Developments in the law of corporate governance

A publication of Nixon Peabody LLP

August 11, 2010

The role and construction of risk committees

By John C. Partigan and Daniel McAvoy

An emerging trend among public companies and some private companies has been the formation of stand-alone risk committees of the board of directors. While most of these are in the financial services or insurance industry, an increasing number of public companies in other industries have been instituting risk committees.¹ In addition, the recently enacted Dodd-Frank Wall Street Reform and Consumer Protection Act (the “Dodd-Frank Act”), requires banks with greater than \$10 billion of consolidated assets, as well as certain nonbank financial companies supervised by the Board of Governors of the Federal Reserve Bank, to establish stand-alone risk committees of the board of directors.²

The purpose of this article is to explore the general legal framework for risk oversight by the board of directors, the pros and cons of establishing a stand-alone risk committee, and to suggest how a risk committee can be configured to ensure its maximum effectiveness.

Legal framework for risk oversight by boards of directors

One of the duties of the board of directors of a Delaware corporation is to provide oversight of the company’s risk management.³ Additional risk oversight and related disclosure obligations arise under the federal securities laws and applicable stock exchange listing standards.

The Delaware courts have held that the board’s fiduciary duties include a duty to attempt in good faith to oversee and monitor the operation of the company’s reporting or information systems designed to identify risks, including violations of laws or regulations.⁴ The board is subject to liability for a failure in such oversight and monitoring where there is “a sustained or systematic failure to exercise oversight” or “[a]n utter failure to attempt to ensure a reporting and information system [has been implemented].”⁵ The Delaware courts have recently reiterated that while this duty exists, there is an extremely high burden for a plaintiff to bring a claim for director liability for failing to monitor the company’s risks.⁶ Companies should implement appropriate risk reporting and monitoring systems, and review these systems on a regular basis, to avoid the possibility of director liability under this line of cases.

Additional risk management responsibilities were imposed on boards with the passage of the

Sarbanes-Oxley Act of 2002. These responsibilities relate, in part, to the establishment and monitoring of policies and procedures for the preparation of the company's financial statements and the reports that it files with the SEC. One major change that related directly to risk management was the requirement that the company disclose any material weakness in the company's internal control over financial reporting. Another important change was the requirement that the principal executive officer and principal financial officer of each public company certify as to the effectiveness of the company's internal controls. A commonly used framework for establishing and monitoring these internal controls is the "Enterprise Risk Management–Integrated Framework," a framework released by the Committee of Sponsoring Organizations of the Treadway Commission.⁷ Under the COSO Integrated Framework, the company's goal is to develop policies and procedures that will not only allow the company to make the required internal control disclosures and its officers to make the required certifications, but also that will strengthen the company's overall enterprise risk management.⁸

The SEC has long required public companies to disclose the most significant risks relating to the ownership of the company's securities.⁹ In addition, most public companies are required to disclose a qualitative and quantitative analysis of exposures to market risk.¹⁰ The SEC recently added a number of required proxy disclosures that touch upon risk, and thus require a company to evaluate those risks. First, many public companies now include a narrative disclosure of the company's compensation policies and practices as they relate to the company's risk management practices.¹¹ This requires a disclosure of the company's policies and practices of compensating its employees and management as they relate to risk, to the extent that risks arising from these compensation policies are reasonably likely to have a material adverse effect on the company. While not required, many companies disclose risk-related compensation policies even where those policies would not likely result in a material adverse effect.¹² Second, most public companies are required to disclose the extent of the board's role in risk oversight, such as how the board administers that oversight function and the effect that this has on the board's leadership structure.¹³ This disclosure is intended to provide investors with information on how a company perceives the role of its board and the relationship between the board and senior management in managing the material risks of the company.¹⁴

In addition, the New York Stock Exchange ("NYSE") corporate governance rules require audit committees of listed companies to perform certain risk oversight duties.¹⁵ A listed company's audit committee is required to discuss policies with respect to risk assessment and risk management.¹⁶ The commentary to the rules provides that while it is management's responsibility to assess and manage risks, the audit committee must discuss the guidelines and policies to govern the process by which that assessment and management is handled.¹⁷ Furthermore, the audit committee is not required to be the sole body responsible for oversight of risk management and assessment, but the audit committee must discuss guidelines and policies to govern the process by which risk assessment and risk management are taken. These rules do not preclude the formation of a separate risk committee as long as the risk committee's oversight process is reviewed by the audit committee and the audit committee continues to perform the duties required by the NYSE rules.

While a number of public and some private companies have already formed risk committees, the Dodd-Frank Act has created the first U.S. statutory requirement to form a risk committee.¹⁸ Under the Dodd-Frank Act, the Board of Governors of the Federal Reserve Board has been directed to issue regulations requiring each bank holding company with consolidated assets of greater than \$10 billion, as well as each nonbank financial company supervised by the Board of Governors, to

establish a risk committee. In addition, the Dodd-Frank Act gives the Board of Governors latitude to create regulations that would require smaller bank holding companies to institute risk committees. The risk committee will be responsible for oversight of the enterprise-wide risk management practices of the company. Similar to the concept of an “audit committee financial expert” for audit committees,¹⁹ such a risk committee must have at least one risk management expert with experience identifying, assessing, and managing risk exposures of large, complex firms. Furthermore, the Board of Governors was directed to enact independence requirements for the members of the risk committee.

In addition to the Dodd-Frank Act, at least two other bills have been introduced in Congress that would impose even stricter risk management requirements upon boards of directors, including one that would require all public companies to establish a risk committee comprised entirely of independent directors.²⁰ In addition, it is likely that public companies will see more frequent shareholder action in the future pertaining to risk management. Until recently, a company could exclude shareholder proposals relating to the subject of risk under the theory that it was an ordinary business matter. In late 2009, the SEC staff released a legal bulletin clarifying that the staff may not routinely grant exclusions for shareholder proposals relating to risk if the proposal raises significant policy issues and there is a sufficient nexus between the nature of the proposal and the company.²¹ The staff also stated in the legal bulletin that “we note 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.”²²

The role of risk committees

As noted above, it is the responsibility of the board of directors to provide oversight of the company’s risk management systems. A risk committee would not supplant the oversight role of the board of directors; rather, the creation of a risk committee is a means of assisting the board in exercising those duties.

Risk management can mean different things to different companies. For some companies, risk management means taking only measured and informed risks in order to avoid loss. For others, it means creating policies that encourage the company to take enough risks to create additional value, but not so much risk that the company loses value. The goals of the company’s risk management may color its risk management policies, whether it forms a risk committee, and the duties of that risk committee.

Certain possible duties of a stand-alone risk committee, especially for non-financial services companies, may include:

- Determining the most important of the company’s operational risks, including identifying any potentially catastrophic risks
- Making recommendations to the board of directors with respect to the amount of risk-taking activity in which the company should engage on an enterprise-wide level
- Overseeing company-wide risk management practices
- Establishing qualitative and quantitative risk and reward goals and monitoring key risks on a regular basis

- Reviewing the company’s periodic reports to ensure proper disclosure of risks and risk factors
- Reviewing systems of communication, both vertically and horizontally, to ensure the proper flow of information related to risks

Potential benefits and drawbacks of risk committees

When a board is evaluating risk management issues, one point to consider is whether the board should form a separate committee devoted to risk. There is no ‘one size fits all’ approach to risk management, and the methods by which a company may choose to assess, manage, and provide oversight of its risks can differ from company to company. If a change is not mandated by the Dodd-Frank Act or other laws or listing standards that may be adopted in the future, a company may make this decision based on numerous considerations, including the level of overall operational risk and the complexity of managing those risks, the company’s appetite for risk and its ability to tolerate losses, whether the company is engaging in riskier and more aggressive strategies to increase shareholder value, the company’s growth strategy, and whether the company is seeking to improve its credit rating.²³

A number of considerations could lead the board to conclude that a separate risk committee should be established. While the list below is not exhaustive, some important benefits of having a stand-alone risk committee may include the following:

- *Setting the tone for a corporate culture of risk management.* Creation of a stand-alone risk committee can help inform both investors and employees that the company is serious about risk management issues. Further, a smaller group of directors focused primarily on risk management may be better able to conceive strategies and general objectives, and make allocations of resources, that tie into the company’s enterprise risk management.
- *Increasing the overall level of enterprise risk management.* A risk committee can enable the board to devote more attention to risk, by making risk management the primary focus of these directors during committee meetings. In addition, this may give management an opportunity to perform risk assessments and provide regular reports on risk-related issues. The theory from a governance perspective is that the risk committee will be a standing committee with an ongoing agenda, and that risk management will become the primary agenda focus, not simply another topic on the list. This approach may be particularly important for companies with more complex risk management issues.
- *Additional expertise in managing operational risks.* If there is a body for which the sole focus is risk, that body may be able to come to a more nuanced understanding of the operational and other risks facing the company. Also, with the additional time devoted to risk issues by certain board members, the committee may be able to develop specific risk management expertise and better communicate to management the means and strategies to mitigate risks.
- *Additional devotion to risk oversight without significantly increasing responsibilities of the entire board.* Boards of directors and audit committees may already devote a significant amount of time to risk oversight. Allowing these risks to be first discussed in a more controlled setting may create additional time for the board, the audit committee, and the compensation committee

to discuss unrelated matters, while giving those bodies a more well-defined understanding of risks as previously developed by the risk committee.

- *Having directors maintain a continuous view of risks.* The nature of the company's operational and other risks frequently changes over time. Having a continuous risk dialogue can help the board better understand subtle changes to the company's risk profile, as well as help the board better identify emerging risks and risks that may be inherent in new or existing operations.
- *Increasing communication processes regarding risks.* A risk committee can serve as a singular unit to which management can report risk-taking activity and the emergence of new risks on a regular basis. Since the committee is designed specifically to focus on risks, risk management employees should be able to bring issues to the committee with their undivided attention. In addition, the members of the committee can serve as an effective liaison between the company's risk management coordinators and the board as a whole.

On the other hand, there may be drawbacks to having a stand-alone risk committee:

- *Increased demands on director time.* Some organizations, especially those with smaller boards of directors, may find that their directors are already strained for time. Adding one more committee means that the company will need to assign directors to serve on that committee, which might not be feasible for companies whose board members are already serving on multiple committees. This concern can be exacerbated if the company requires the members of each of its committees to be independent directors.
- *Increased organizational costs.* Typically, a public company will pay directors for attendance at board and committee meetings. An additional committee and committee chair means additional compensation to the directors serving on that committee. Furthermore, an additional level of process can mean other added organizational costs.
- *Potential duplication of duties.* Unless the charter of the risk committee is well constructed in the context of other committees and the board as a whole, there is great potential for the risk committee to duplicate many of the duties of the audit committee and compensation committee. In addition, even if a company has a stand-alone risk committee, the audit committees of NYSE-listed companies will still be required to provide a certain level of risk oversight, as described above.
- *Current effective risk management.* The board of directors may determine that the current level of the company's risk management is sufficient to meet the company's needs. Certain companies with low risk profiles may already have sufficient oversight of risk management under the existing processes of the board and the audit committee. Some of the ways in which the committee could mitigate these issues are discussed below under the heading "Interplay between risk committees, the board and management."
- *Need to set additional internal processes.* Even if the board establishes a stand-alone risk committee, the committee may not be able to effectively provide oversight of enterprise risks if processes are not put in place to ensure that the committee is informed of risky activities and other corporate risks. In addition, lines of communication would need to be established between the risk committee, the board of directors as a whole, and the other committees of the board to ensure that those other bodies are able to incorporate the

analysis of the company's risks into the performance of their duties. Some of the ways in which the committee could mitigate these issues are discussed below under the heading "Interplay between risk committees, the board and management."

Interplay between risk committees, the board, and management

If the board of directors determines to establish a separate risk committee, one of the key considerations for counsel establishing the committee structure and charter will be ensuring that the risk committee functions properly within the context of the rest of the board and management, and to ensure that there is not significant overlapping of duties between the risk committee and the other board committees. The following are certain considerations to make in the construction of a risk committee:

- While the charter of a new risk committee is being drafted, the company may wish to consider also amending the charters of the audit committee and compensation committee. If properly drafted and revised, the charters should minimize overlap between the duties of the committees while specifying the areas in which the committees, management, and the board as a whole will need to interact to formulate cohesive strategies and implement an enterprise risk management system that permeates all levels of the company.
- The risk committee should have one member who is also on the audit committee, and possibly one member who is also on the compensation committee. Certain responsibilities of the two committees will inherently overlap, especially with respect to risks that can affect results of operations and risk-taking activity that may be promoted by company-wide compensation policies. Having common members can help the committees as a whole to recognize the areas of this overlap, help formulate plans and policies from a wider perspective, and prevent duplication of duties between the committees. Due to the particularly close relationship between audit committee responsibilities and risk committee responsibilities, some companies may wish to take this even one step further and have the chairman of the audit committee serve as assistant chairman of the risk committee and vice versa.
- While the members of the risk committee ideally would be independent, it is important to have mechanisms to ensure open communication, both with the board of directors and the company's chief risk officer, or other officers, in charge of risk management. The committee may wish to have executive sessions with risk management employees, much in the same way the audit committee would have executive sessions with the company's independent outside auditors.
- When recruiting director nominees and committee members, the company may wish to take risk management experience into account. Not only will this help ensure that the committee is well equipped to evaluate the company's risks, but it would also help provide a fuller picture of the company to investors in the company's required disclosures regarding director qualifications and the role of diversity in selecting board nominees.²⁴
- If the company is listed on the NYSE, the audit committee is still required to discuss policies with respect to risk assessment and risk management; however, the risk committee could be used to assist the audit committee in performing these duties. For example, in some

committee charters, the risk committee is required to bring to the audit committee for discussion at a joint session any items that have a significant financial statement impact or require significant financial statement or regulatory disclosures. This is a helpful feature since it allows the risk committee to be more focused on risk assessment, but then brings the two committees together if a material issue arises.

What is best for your company?

As a result of the increased focus on risk in many public companies, and the likelihood that this trend will continue in the future as a result of recent legislative changes and administrative actions, directors and their counsel should consider the need for and potential benefits of establishing a stand-alone risk committee. They should review both the potential benefits and concerns before making a decision to create a risk committee. If they decide that a risk committee may be beneficial, the structure, role, and activities of the committee should be carefully considered, in view of the legal framework for risk oversight by the board of directors and the potentially overlapping responsibilities of the audit and compensation committees, in order to maximize its effectiveness.

Contact us

For more information regarding this Alert or if you have any questions, please reach out to your regular Nixon Peabody attorney or:

- In our Boston office, William E. Kelly, at 617-345-1195 or wkelly@nixonpeabody.com
- In our New York office, Daniel McAvoy, at 212-940-3112 or dmcavoy@nixonpeabody.com
- In our Rochester office, Deborah J. McLean, at 585-263-1307 or dmclean@nixonpeabody.com
- In our San Francisco office, Steven M. Plevin, at 415-984-8462 or splevin@nixonpeabody.com
- In our Washington D.C. office, John C. Partigan, at 202-585-8535 or jpartigan@nixonpeabody.com and Raymond J. Gustini, at 202-585-8725 or rgustini@nixonpeabody.com

1 Non-bank companies that have instituted stand-alone risk committees include La-Z-Boy
Incorporated (household furniture); CA, Inc. (information technology software); Duke Energy
Corp. (electric services); and Regency Energy Partners LP (natural gas processing), among
numerous others.

2 Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203 §165(h)
(2010).

3 *In re Caremark Int'l Inc. Derivative Litigation*, 698 A.2d 959 (Del. Ch. 1996).

4 *Id.* at 967–968.

5 *Id.* at 971.

6 *See, e.g., Lyondell Chem. Co. v. Ryan*, 970 A.2d 235, 241 (Del. 2009); *In re Citigroup Inc.*
S'holder Derivative Litig., 964 A.2d 106 (Del. Ch. 2009).

7 COSO, *Enterprise Risk Management–Integrated Framework* (2004).

8 COSO, *Strengthening Enterprise Risk Management for Strategic Advantage* at 4 (2009), available
at http://www.coso.org/documents/COSO_09_board_position_final102309PRINTandWEBFINAL.pdf.

9 *See* Item 503(c) of Regulation S-K. 17 CFR § 229.503(c).

10 *See* Item 305 of Regulation S-K. 17 CFR § 229.305.

11 *See* Item 402(s) of Regulation S-K. 17 CFR § 229.402(s).

12 *See, e.g.,* RiskMetrics Group U.S. Proxy Disclosure Requirements FAQ, available at
http://www.riskmetrics.com/policy/2010_NewUSDisclosureFAQ (stating that while RiskMetrics Group does
not have a policy regarding non-disclosure, they advise issuers to, at a minimum, talk about their
process and any mitigating features that they have adopted).

13 *See* Item 407(h) of Regulation S-K. 17 CFR § 229.407(h).

14 SEC Securities Act Release No. 33-9052, *Proxy Disclosure and Solicitation Enhancements* at 35
(July 10, 2009).

15 While the NASDAQ rules do require listed companies to form an audit committee with an audit
committee charter, the NASDAQ rules do not specifically require risk oversight to be a duty of the
audit committee enunciated in the audit committee charter. NASDAQ Rule 5605; NASDAQ IM-
5605-3.

16 NYSE Listed Company Manual 303A.07(b).

17 *Id.*

18 Dodd-Frank Act at § 165(h).

19 *See, e.g.,* Item 407(d)(5) of Regulation S-K. 17 CFR § 229.407(d)(5).

20 Shareholders Bill of Rights Act of 2009, S. 1074, 111th Cong. (2009). *See also* Shareholder
Empowerment Act of 2009, H.R. 2961, 111th Cong. (2009).

21 Staff Legal Bulletin No. 14E (CF), October 27, 2009.

22 *Id.*

23 Standard & Poor's and Moody's both use evaluations of enterprise risk management in making
their determinations for a company's credit ratings. *See* <http://www.standardandpoors.com/ratings/erm/en/us>
for Standard & Poor's philosophy on enterprise risk management, and
[http://www.moodys.com/cust/content/loadcontent.aspx?source=staticcontent/Free%20Pages/Regulatory%20Affairs/RMP.h](http://www.moodys.com/cust/content/loadcontent.aspx?source=staticcontent/Free%20Pages/Regulatory%20Affairs/RMP.htm)
[tm](http://www.moodys.com/cust/content/loadcontent.aspx?source=staticcontent/Free%20Pages/Regulatory%20Affairs/RMP.htm) for Moody's rating methodologies.

24 Recent amendments to the proxy rules require disclosure of (i) the specific experience,
qualifications, attributes, or skills that led to the conclusion that a board nominee should serve as a
director and (ii) how the nominating committee (or board) considered diversity in identifying
nominees for director, including diversity of experience. *See* Items 401(e)(i) and 407(c)(2)(vi) of
Regulation S-K. 17 CFR § 229.401(e)(1); 17 CFR § 229.407(c)(2)(vi).