

Corporate Alert

The Board's Role in Risk Oversight: A Survey of Recent Proxy Statement Disclosures

April 6, 2010

New Securities and Exchange Commission (SEC) disclosure rules require companies to describe in their proxy statements the role of the board of directors in overseeing risk management. To find out what companies are saying in response to the new requirement, we reviewed the disclosures in proxy statements filed by 50 S&P 500 companies since the February 28, 2010 effective date of the new rules. In this alert, we discuss the legal and regulatory underpinnings of the board's role in risk oversight, the increasing use by companies of an enterprise-wide approach to risk management and, finally, the results of our review.

The Board's Role In Risk Oversight

In general, the board of directors is obligated to oversee the company's risk management processes and controls, while management is charged with the day-to-day management of the company's risks. There are several state law and regulatory requirements that relate to the board's role in risk management oversight:

- **Fiduciary Duties.** Under Delaware law, directors have a duty of oversight that requires them to implement and oversee the operation of reasonable information and reporting systems or controls designed to inform them of material risks.¹ Directors will not be held liable, however, for breach of their oversight duty unless they acted in bad faith by either completely failing to implement any information and reporting systems or, having implemented such a system, consciously failing to monitor or oversee its operations or warnings it provides.²

Two Delaware court decisions handed down in 2009 expound on this duty of oversight. In the first case, the Delaware Chancery Court allowed claims against several AIG directors (who were also insiders) to proceed where it was claimed that the defendants knowingly failed to properly monitor alleged pervasive fraudulent and criminal conduct by AIG employees.³ The AIG decision is one of the few cases in which plaintiffs were able to survive motions to dismiss claims against directors for breach of the duty to oversee their company's legal compliance systems. All of these cases involved allegations of fairly egregious conduct in which directors utterly failed to implement a monitoring system or ignored numerous "red flag" warning signs of employee misconduct.⁴

In the second 2009 decision, the Delaware Chancery Court dismissed claims against the directors of Citigroup for alleged failures to properly monitor and manage the risks associated with Citigroup's exposure to the subprime mortgage crisis.⁵ In dismissing the claims, the court clarified that the duty of oversight is not designed to subject directors to personal liability for failure to predict the future and to properly evaluate *business* risk. The mere fact that a company takes on business risk and suffers losses—even catastrophic losses—does not establish bad faith. The court noted that the plaintiffs conceded that Citigroup had procedures and controls in place to monitor risk, including having a board

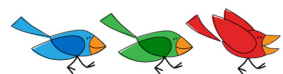
¹ See *Stone v. Ritter*, 911 A.2d 362 (Del. 2006).

² *Id.*

³ *American International Group, Inc. Consolidated Derivative Litigation*, 2009 WL 366613 (Del. Ch. 2009).

⁴ See, e.g., *In re Caremark Int'l Inc. Derivative Litigation*, 69 A.2d 959 (Del. Ch. 1996).

⁵ *In re Citigroup Shareholder Derivative Litigation*, 2009 WL 481906 (Del. Ch. Feb. 24, 2009).



www.twitter.com/akin_gump

committee that was expressly charged with assisting the board in fulfilling its oversight responsibility with respect to risk management, which committee had met at least 11 times during the period in question.

While it is clear that Delaware courts will not second-guess directors in assessing and taking business risks on behalf of the enterprise, directors should, nevertheless, remain vigilant in monitoring their company's business risks. In addition to heightened shareholder and regulatory scrutiny, the financial crisis and severe recession of the past few years have demonstrated that more diligent risk management is not merely a "best" practice, but also a necessary practice to ensure survival of the enterprise.

- **Stock exchange requirements.** In addition to the board's fiduciary duties under state law, NYSE listing standards require audit committees of listed companies to discuss the company's guidelines and policies regarding risk assessment and risk management, as well as the company's major financial risks and the steps management has taken to monitor and control those risks.⁶ Under the NYSE rules, however, the audit committee is not required to be the sole body responsible for risk management and assessment. If other mechanisms are used, the audit committee should review such processes in a general manner.⁷
- **Federal sentencing guidelines.** Under federal sentencing guidelines, a business organization can reduce potential penalties (and perhaps avoid prosecution altogether) for wrongdoing if the organization can demonstrate that it had an effective compliance program. The guidelines require that directors exercise reasonable oversight over the implementation and effectiveness of the compliance program to ensure that it is generally effective in preventing and detecting criminal conduct. The guidelines also specifically require that directors receive appropriate training as to their roles and responsibilities.
- **SEC requirements.** New SEC disclosure rules that went into effect February 28, 2010, require companies to describe in their proxy statements the role of the board of directors in overseeing risk management. Specifically, a company must "disclose the extent of the board's role in risk oversight of the registrant, such as how the board administers its oversight function, and the effect that this has on the board's leadership structure."⁸ In the adopting release, the SEC explained that "disclosure about the board's involvement in the oversight of the risk management process should provide important information to investors about how a company perceives the role of its board and the relationship between the board and senior management in managing the material risks facing the company."⁹ The SEC suggested that, where relevant, companies disclose whether the officers responsible for risk management report directly to the board or to a board committee or how the board or committee otherwise receives information from such persons.¹⁰

The new SEC disclosure rules also require companies to explain how their compensation policies and practices for employees affect the company's risks and risk management if the risks arising from these policies and practices are reasonably likely to have a material adverse effect on the company.¹¹

In addition to the new SEC disclosure requirements, the Sarbanes-Oxley Act requires public companies to, among other things, assess the effectiveness of their internal control over financial reporting, maintain disclosure controls and procedures and provide direct audit committee oversight of the independent auditors. In addition, SEC rules adopted in 2005 require companies to disclose in their annual reports on Form 10-K all material risks and to disclose any material changes to those risks in a Form 10-Q.

- **TARP.** Companies participating in the Capital Purchase Program under the Troubled Asset Relief Program (TARP) are required to take certain steps to ensure that incentive compensation for senior executives does not encourage unnecessary and excessive risks that threaten the value of the enterprise. Among other things, the compensation committee must review the compensation arrangements for senior executives to ensure that such arrangements do not encourage unnecessary or excessive risks. A certification that such reviews have taken place must be included in the company's proxy statement as part of the compensation committee's report.

⁶ NYSE Listed Company Manual § 303A.07(c)(iii)(D) and related Commentary.

⁷ Commentary to NYSE Listed Company Manual § 303A.07(c)(iii)(D).

⁸ Regulation S-K Item 407(h).

⁹ SEC Release Nos. 33-9089; 34-61175, Proxy Disclosure Enhancements (December 16, 2009) at p. 44.

¹⁰ *Id.*

¹¹ Regulation S-K Item 402(s).

Enterprise Risk Management

In the wake of the financial crisis, many companies have implemented more comprehensive and integrated risk management programs, and boards of directors have expanded their risk oversight to encompass not just the legal and financial risks that audit committees have traditionally overseen, but also the full panoply of risks that a company may face. Enterprise risk management (ERM) is the current buzzword applied to a top-down holistic approach to risk management. It addresses all of an enterprise's risks—including operational, financial, strategic, compliance and reputational risks—under one umbrella, in contrast to the more traditional “silo” approach in which each operating function or division tackled risk independently. ERM is not focused simply on risk reduction. Rather, it encompasses an assessment of both upside and downside risks and, thus, helps inform the strategic planning process. Indeed, to make informed decisions about the company's strategic direction, the board must have a full understanding of all of the major risks involved.

There are several frameworks available to assist companies in implementing ERM.¹² In addition, two leading organizations recently issued helpful guidance for boards of directors to steer them through their risk oversight duties.¹³ One of them, the Committee of Sponsoring Organizations of the Treadway Commission (known as COSO) has identified four areas of board focus in enterprise risk management:¹⁴

- Understand the company's risk philosophy and concur with the company's “risk appetite,” that is, the amount of risk that the company is willing to accept in pursuit of stakeholder value.
- Know the extent to which management has established effective risk management processes that identify, assess and manage the company's most significant enterprise-wide risks.
- Review the company's risk portfolio in relation to the agreed risk appetite, including through strategic and operational initiatives that integrate enterprise-wide risk exposures.
- Be apprised of the most significant risks and whether management is responding appropriately.

Survey Of Risk Oversight Disclosures

To assess the types of disclosures that companies are providing about the board's role in overseeing risk management, we reviewed preliminary or final proxy statements filed by 50 randomly selected S&P 500 companies since the February 28, 2010 effective date of the new disclosure rules. The results of our survey, categorized by the various types of disclosures, are set forth below.

Separate Section Devoted to Risk Oversight

Ninety-two percent of surveyed companies had a designated section in their proxy statements for risk oversight. This section typically stood alone, but sometimes was combined with the section addressing board leadership structure. Typically, the section was located in the portion of the proxy statement discussing corporate governance matters and was often titled “The Board's Role in Risk Oversight” (or words of similar effect).

Statements about Management's Primary Risk Management Responsibility

Twenty-four percent of surveyed companies included a statement to the effect that management is primarily responsible for risk management, while the board's role is one of oversight.

¹² See, e.g., the ERM framework adopted by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), available at http://www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf. See also The Conference Board, “Emerging Governance Practices in Enterprise Risk Management” (Feb. 2007).

¹³ COSO, “Effective Enterprise Risk Oversight, The Role of the Board of Directors 2009,” available at www.coso.org; National Association of Corporate Directors, Blue Ribbon Commission Report on Risk Governance: Balancing Risk and Reward (2009).

¹⁴ *Id.*

Sample disclosures are set forth below:

Sunoco, Inc.: “Management of risk is the direct responsibility of the Company’s CEO and the senior leadership team. The Board has oversight responsibility, focusing on the adequacy of the Company’s enterprise risk management and risk mitigation processes.”

Peabody Energy Corporation: “Management is responsible for the day-to-day management of the risks we face, while the Board, as a whole and through its committees, has responsibility for the oversight of risk management.”

AT&T Inc.: “Assessing and managing risk is the responsibility of the management of AT&T. The Board of Directors oversees and reviews certain aspects of the Company’s risk management efforts.”

Strategic Direction

Forty-two percent of surveyed companies explained that oversight of risk management was an important or integral part of the board’s role in the strategic planning process.

Several illustrative examples are set forth below:

Valero Energy Corporation: “The Board also believes that risk management is an integral part of Valero’s annual strategic planning process, which addresses, among other things, the risks and opportunities facing Valero.”

Stryker Corporation: “A fundamental part of setting the Company’s business strategy is the assessment of the risks the Company faces and how they are managed.”

Bristol-Myers Squibb Company: “Our Board meets regularly to discuss the strategic direction and the issues and opportunities facing our company in light of trends and developments in the biopharmaceutical industry and general business environment. Our Board has been instrumental in determining our strategy to combine the best of biotechnology with pharmaceuticals to become a best-in-class next generation biopharmaceutical company. Throughout the year, our Board provides guidance to management regarding our strategy and helps to refine our operating plans to implement our strategy. Each year, typically during the second quarter, the Board holds an extensive meeting with senior management dedicated to discussing and reviewing our long-term operating plans and overall corporate strategy. A discussion of key risks to the plans and strategy as well as risk mitigation plans and activities is led by the Chairman and Chief Executive Officer as part of the meeting. The involvement of the Board in setting our business strategy is critical to the determination of the types and appropriate levels of risk undertaken by the company.”

Enterprise Risk Management

Fifty-four percent of surveyed companies expressly used the term “enterprise risk management.”

Sample disclosures are set forth below:

American Express Company: “The Company relies on its comprehensive enterprise risk management process (ERM) to aggregate, monitor, measure and manage risks. The ERM approach is designed to enable the Board of Directors to establish a mutual understanding with management of the effectiveness of the Company’s risk management practices and capabilities, to review the Company’s risk exposure and to elevate certain key risks for discussion at the Board level. The Company’s ERM program is overseen by its Chief Risk Officer who is an executive officer of the Company and a member of the Company’s most senior management.”

Express Scripts, Inc.: “In order to assist the board of directors in overseeing our risk management, we use enterprise risk management (“ERM”), a company-wide initiative that involves the board of directors, management and other personnel in an integrated effort to identify, assess and manage risks that may affect our ability to execute on our corporate strategy and fulfill our business objectives. These activities entail the identification, prioritization and assessment of a broad range of risks (e.g., financial, operational, business, reputational, governance and managerial), and the formulation of plans to manage these risks or mitigate their effects.”

Primary Responsibility at Board vs. Committee Level

Eight percent of surveyed companies stated that the primary responsibility for risk management oversight rests with the entire board, 34 percent of surveyed companies stated that primary responsibility is vested in one or more committees and 52 percent reflected that both the board and various committees have responsibility for risk management oversight.

Of those companies where primary responsibility is vested in one or more committees, 65 percent (22 percent of all surveyed companies) identified their audit committees as having primary responsibility, 18 percent had a separate committee expressly dedicated to risk management (all of these companies were in the financial services or insurance industries) and 18 percent stated that various board committees were responsible for overseeing the management of risks relating to the committee's primary areas of responsibility.

Regardless of where primary responsibility rested, over half of the surveyed companies included descriptions of the specific types of risks that various committees of the board oversee.

Compensation Committee Responsibility for Determining Compensation Risk Disclosure

As discussed above, the new SEC disclosure rules require companies to discuss their compensation policies and practices for employees as they relate to risk management practices and risk-taking incentives if the risks arising from those policies and practices are reasonably likely to have a material adverse effect on the company. The new rules do not require a company to include any disclosure if the company has determined that the risks arising from its compensation policies and practices are not reasonably likely to have a material adverse effect. RiskMetrics has announced that it does not take a position regarding whether companies should disclose their risk determinations where the company has determined that a material adverse effect is not reasonably likely. RiskMetrics does, however, advise companies "at a minimum" to discuss their process in reaching a determination and any mitigating features (such as clawbacks or bonus banks) that they have already adopted.¹⁵ RiskMetrics views this disclosure "as an opportunity for communication, not simply compliance" and expects that shareholders will be looking for a reasonably substantive discussion of the board's process for determining whether the company's incentive pay programs motivate inappropriate risk-taking and what they are doing to mitigate that risk.

Our survey shows that many companies elected to provide disclosure about their compensation risk determinations and the process the company undertook to make the determination.

- **Compensation Committee Responsibility to Assess Risks.** Sixty-eight percent of surveyed companies stated that their compensation committee was charged with either determining that the compensation policies and practices do not encourage excessive risk-taking or determining whether the risks arising from such policies and practices are reasonably likely to have a material adverse effect on the company.
- **Disclosure of Determination.** Seventy-four percent of surveyed companies expressed a determination that their compensation policies and practices either did not encourage excessive or unnecessary risk-taking (or used words of similar effect) or were not reasonably likely to result in a material adverse effect on the company. Of the 37 companies that disclosed a determination, 17 of them (46 percent) phrased their conclusion in terms of the absence of a material adverse effect, 15 companies (41 percent) expressed their conclusion in terms of not encouraging excessive or unnecessary risk-taking and the remaining companies phrased their conclusions in terms of a determination of an "appropriate level of risk-taking" or an "effective balance of risk and reward" or words of similar effect.
- **Who Made the Determination.** Companies varied widely as to who made the risk determination regarding compensation programs and policies. Twenty-three companies (62 percent of those disclosing the determination) stated that the determination was made by the compensation committee, 10 companies (27 percent of those disclosing the determination) phrased the determination as being made by the company or "we" and, in the remaining instances, "management" made the determinations.
- **Process for Determination.** Sixty-five percent of those companies disclosing a risk determination provided disclosure of the process that the company or compensation committee undertook to make the determination.

¹⁵ See RiskMetrics Group, "US Proxy Disclosure Requirements: FAQ."

- **Location of Determination.** Companies varied widely on the location of the disclosure in their proxy statements. Almost half of the companies included the disclosure in Compensation Discussion and Analysis. Other popular disclosure locations included under a separate heading in the corporate governance section, in the discussion of board oversight of risk or under a separate heading near discussions of compensation committee interlocks and compensation consultants.
- **Risk-Mitigating Features.** Regardless of whether a company disclosed a risk determination with respect to its compensation policies and practices, almost three-quarters of the surveyed companies discussed various features of their compensation programs and policies that are designed to mitigate excessive risk-taking.

The following excerpt from Kraft Foods' proxy statement discusses the compensation committee's process in evaluating compensation risks, risk-mitigating features contained in the company's compensation policies and practices and the conclusion of the compensation committee with respect to such risks:

"Analysis of Risk in the Compensation Architecture"

In 2009, the Human Resources and Compensation Committee evaluated the current risk profile of our executive and broad-based compensation programs. In its evaluation, the Human Resources and Compensation Committee reviewed the executive compensation structure and noted numerous ways in which risk is effectively managed or mitigated. This evaluation covered a wide range of practices and policies including: the balance of corporate and business unit weighting in incentive plans, the balanced mix between short-term and long-term incentives, caps on incentives, use of multiple performance measures, discretion on individual awards, a portfolio of long-term incentives, use of stock ownership guidelines, and the existence of anti-hedging and clawback policies. In addition, the Human Resources and Compensation Committee analyzed the overall enterprise risks and how compensation programs impacted individual behavior that could exacerbate these enterprise risks. The Human Resources and Compensation Committee collaborated with the Audit Committee in this analysis. Additionally, we engaged an outside independent consultant to review our incentive plans (executive and broad-based) to determine if any practices might encourage excessive risk taking on the part of senior executives. The outside consultant noted several of the practices of our incentive plans (executive and broad-based) that mitigate risk, including the use of multiple measures in our annual and long-term incentive plans, Human Resources and Compensation Committee discretion in payment of incentives in the executive plans, use of multiple types of long-term incentives, payment caps, significant stock ownership guidelines, and our recoupment and anti-hedging policies. In light of these analyses, the Human Resources and Compensation Committee believes that the architecture of Kraft Foods' compensation programs (executive and broad-based) provide multiple, effective safeguards to protect against undue risk."

Reporting Processes

As previously discussed, the SEC suggested in the adopting release that, where relevant, companies disclose in their proxy statements whether the officers responsible for risk management report directly to the board or to a board committee or how information is otherwise received from such persons. Thirty-eight percent of surveyed companies identified their principal risk officer or officers by title and disclosed that the officer or officers reported directly to the board or a board committee.

Frequency of Entire Board Review

One-third of surveyed companies reported that the full board reviews risk management at least annually, 22 percent stated that the full board reviews risk management issues "periodically" or "regularly" and a few companies reported quarterly or semiannual reviews by the entire board.

Length of Disclosure

Most companies devoted at least two or three paragraphs to their discussion of the board's role in risk oversight. The average length of the disclosures was 10 sentences, with the length of the discussion ranging from a high of 27 sentences to a low of three sentences. These numbers do not reflect any specific discussions of risks relating to compensation policies and practices or factors mitigating those risks.

Effect of Board's Role in Risk Oversight on Leadership Structure

Only 20 percent of the surveyed companies specifically addressed the effect of the board's role in risk oversight on the board's leadership structure. Instead, most companies simply stressed in the discussion of their leadership structure the role that a lead director or the independent directors play in providing strong, effective oversight of management.

Set forth below are disclosures by several companies that expressly addressed the matter:

IBM: "The Board's role in risk oversight of the Company is consistent with the Company's leadership structure, with the CEO and other members of senior management having responsibility for assessing and managing the Company's risk exposure, and the Board and its committees providing oversight in connection with those efforts."

Teco Energy: "We believe that our Board leadership structure promotes effective oversight of the company's risk management for the same reasons that we believe the structure is most effective for our company in general, that is, by providing unified leadership through a single person, while allowing for input from our independent Board members, all of whom are fully engaged in Board deliberations and decisions."

The Coca-Cola Company: "The Company believes that its leadership structure, discussed in detail [above], supports the risk oversight function of the Board. While the Company has a combined Chairman of the Board and Chief Executive Officer, strong Directors chair the various committees involved in risk oversight, there is open communication between management and Directors, and all Directors are actively involved in the risk oversight function."

Conclusion

Our survey reveals that there are several common themes emerging in the disclosures that companies are making in their proxy statements regarding the board's role in risk oversight. Despite some common elements, however, companies reported a wide range of differences in the manner in which boards and board committees carried out their risk oversight responsibilities, reflecting the fact that disclosure of this critical board task must be specifically tailored to the particular company and the risks it faces.

CONTACT INFORMATION

If you have any questions concerning this alert, please contact —

Patrick J. Hurley
phurley@akingump.com
713.220.8132
Houston

Terry M. Schpok
tschpok@akingump.com
214.969.2870
Dallas

Samuel Wolff
swolff@akingump.com
202.887.4462
Washington, D.C.

Julie M. Kaufer
jkaufer@akingump.com
310.728.3313
Los Angeles

Lucas F. Torres
ltorres@akingump.com
212.872.1016
New York

Ben Morgan
bmorgan@akingump.com
214.969.4218
Dallas