The attached article, Corporate Governance Update: Boards Play a Leading Role In Risk Management Oversight, was published in the New York Law Journal on September 24, 2009.

September 24, 2009

Corporate Governance Update: Boards Play a Leading Role In Risk Management Oversight

David A. Katz
and
Laura A. McIntosh*

One might say that "risk management" is the new "hot topic" in corporate governance. Just as the Enron and other high-profile corporate scandals were seen as resulting from a lack of ethics and oversight, the credit market meltdown and resulting financial crisis have been blamed in large part on inadequate risk management by corporations and their boards of directors.[1] As a result, along with the task of implementing corporate governance procedures and guidelines, a company's board of directors is expected to take a leading role in overseeing risk management structures and policies. What needs to be understood, though, is that there is no way to eliminate risk, nor would any enterprise be well-served by attempting to do so. However, it is important for directors to take steps to be well-informed as to the company's risk profile, to discuss and evaluate risk scenarios and to satisfy themselves on an ongoing basis as to the adequacy of management's efforts to address material risks. The goal should not be to eliminate risk, but to make sure that risks are understood and appropriately managed; the management team is responsible for managing the risks, while the board of directors' role should be one of oversight.[2]

---

* David A. Katz is a partner at Wachtell, Lipton, Rosen & Katz. Laura A. McIntosh is a consulting attorney for the firm. The views expressed are the authors' and do not necessarily represent the views of the partners of Wachtell, Lipton, Rosen & Katz or the firm as a whole.

[1] *See, e.g.*, Clarke Murphy & J. Frank Brown, "Boards Must Take on Risk Management," Business Week, March 17, 2009 ("Failed risk management is at the heart of Wall Street's malaise."); Mark Beasley, "Board and Audit Committee Involvement in Risk Management Oversight," AICPA, Feb. 2, 2009 ("Recent events in the financial markets, including the sub-prime meltdown, continue to highlight the need for improved risk oversight processes for enterprises of all types."), available at http://www.cpa2biz.com/Content/media/PRODUCER_CONTENT/Newsletters/Articles_2009/CPA/Feb/RiskOversight.jsp.

[2] An in-depth review of many issues discussed in this article may be found at Martin Lipton *et al.*, "Risk Management and the Board of Directors," Wachtell, Lipton, Rosen & Katz (WLRK) Publication, November 2008.

If your address changes or if you do not wish to continue receiving these memos, please send an e-mail to Publications@wlrk.com or call 212-403-1487.

Elements of Effective Risk Oversight

There are a number of important elements to risk oversight by a board of directors that can be addressed through effective communication between the board of directors and members of senior management, effective communication among board members, board committees, and board advisors and effective coordination among all of the participants.

Communications between the board of directors and members of senior management. One of the most important elements in effective oversight of risk management is direct communication between members of the board and members of senior management, including senior management executives responsible for risk management. The variety and severity of risks to which a company is exposed, and the extent to which the company can "manage" such risks, depend on many factors, and it is crucial that the board and management share an understanding—which should be updated on an ongoing basis and revised as appropriate—as to the company's overall tolerance for risk. It is the responsibility of management to provide the members of the board with sufficient information to enable them to understand the company's risk profile, including information regarding the external and internal risk environment that the company and its industry face, the specific material risk exposures affecting the company's current and future operations (including financial and other risks), how risks are assessed and prioritized by the management team, risk response strategies, implementation of risk management procedures and infrastructure, and the strength and weaknesses of the overall system. Through effective communications between the board and senior management, members of the board should be confident that the company's executives understand the risks that the enterprise faces and are effective in their day-to-day management of enterprise risk.

Many boards of directors delegate oversight of risk management to the audit committee. Some companies with particularly complex risk management issues choose to establish dedicated risk oversight committees, but this structure is not appropriate for all companies.[3] The board committee charged with risk oversight should have sessions in which they meet directly with the executives primarily responsible for risk management. In addition, directors should create an environment in which senior risk managers and senior executives feel comfortable informing the board or relevant committee of extraordinary risk issues and developments that need the immediate attention of the board outside of the regular board or committee reporting and communication process. As discussed below, it is important in the cases where different board committees may be responsible for different areas of risk oversight (such as the

---

[3] Indeed, relatively few companies currently have separate risk oversight committees. According to the governance research and rating firm GovernanceMetrics International (GMI): of the 4,162 companies covered by GMI globally, only 5.9 percent disclose a stand-alone board-level risk oversight committee or subcommittee. These were most often found among banks and insurance companies. "GMI Looks at Corporate Boards and Risk Oversight," June 29, 2009, available at http://www.gmiratings.com/Release_GMI_Boards_Risk_Oversight_6_29_09.pdf.

audit committee for financial risk, the compensation committee for compensation grants that do not promote undue risk, and a health and safety committee), that the work of these committees be coordinated in a coherent manner so that a consistent level of risk can be maintained and the entire board can be satisfied that it is providing appropriate risk oversight.

Congress is in the process of potentially legislating how boards of directors should deal with risks. The Shareholder Bill of Rights Act of 2009, sponsored by Senators Charles Schumer and Maria Cantwell, would require each public company board of directors to establish a risk committee, comprised entirely of independent directors, which committee would be responsible for the establishment and evaluation of risk management practices. However, a one-size-fits-all formulation would be a mistake—each company must formulate an appropriate process for its board to have oversight of risk management; for some companies, it may be in an audit committee or in a risk committee, and, in other companies, it may be the entire board of directors.

Communications among the board of directors, board committees and board advisors. While the primary board-level risk oversight role often is allocated to a standing committee (such as the audit committee), the full board also should receive information about the company's risk management system and the most significant risks that the company faces. The board committee charged with risk oversight should report on its discussions and findings to the full board on a periodic basis. In addition, the board may choose to receive abbreviated versions of the briefings provided by management and advisors to the committee.

Risk management issues may arise in the context of the work of other committees, and the decision-making in those committees should take into account the company's overall risk management system. For example, the company's compensation structure should be reviewed and, if necessary, revised to avoid incentives that promote excessive risk-taking. Directors would be well-advised to review compensation structures with a view to avoiding compensation awards that might be viewed as encouraging undue risk.[4] Moreover, specialized committees may be tasked with specific areas of risk exposure. Banks, for instance, often maintain credit or finance committees, while energy companies and chemical companies often have public policy board committees largely devoted to environmental and safety issues. It is important that the risk oversight activities of various board committees be coordinated so that a consistent level of risk can be maintained. In addition, the entire board should be informed of the work performed by the various committees responsible for risk oversight so that the entire board of directors can be responsive to changes in a company's risk profile.

If a company keeps the risk oversight function in the audit committee and does not establish a separate risk oversight committee or subcommittee, the audit

---

[4] *See* Martin Lipton & Jeremy L. Goldstein, "Executive Pay and Directors' Duties," WLRK Publication, July 20, 2009.

committee should schedule time for periodic review of risk management outside the context of its role in reviewing financial statements and accounting compliance. While this may further burden the audit committee, it is important to allocate sufficient time on the audit committee agenda to focus on the risk oversight role specifically. The goal should be to permit, through one means or another, serious and thoughtful board-level attention to the company's risk management process and system, the nature of the material risks the company faces, and the adequacy of the company's policies and procedures designed to respond to and mitigate these risks.

Efficient coordination. In order to be certain that each element of risk is being considered and addressed, it is important that the risk management process be kept straightforward and uncluttered by too many participants. A recent report by Ernst & Young on the future of risk management cautions that too many risk management functions can produce an inefficient process, creating significant demands without eliminating coverage gaps or overlapping responsibilities.[5] The report is based largely on a survey of over 500 senior executives. Of the respondents, 73 percent indicated that their company has seven or more risk functions, 67 percent indicated that they had overlapping coverage with two or more risk functions, and 50 percent reported gaps in coverage between risk functions.[6] As noted above, the board of directors and the management team should be in alignment as to the desired risk exposure of the company, and the board should satisfy itself that the management team is communicating its risk management strategy broadly to all appropriate groups within the company so that it is properly integrated into the company's global business strategy.

Expecting the unexpected. A key element of the board of directors' risk oversight function is to discuss and analyze possible risk scenarios with the management team in order to understand how management is appropriately managing the risk management process. In doing so, the board should define risk in broad terms and be willing to imagine highly unlikely scenarios in order to discuss strategies for managing unexpected events. It is not enough to consider only past events or foreseeable contingencies. The board should ask management to compile scenarios for analysis, including some that seem extremely unlikely, and demonstrate the effectiveness of their risk management processes in those situations. The board should be careful to understand and challenge any assumptions underlying management's analyses.[7] The board also should have management review with the board the insurance programs that are in place with the board so that the board can evaluate whether these programs appropriately address the risks that the company faces.

---

[5] Ernst & Young, "The Future of Risk: Protecting and Enabling Performance (2009)", available at http://www.ey.com/Publication/vwLUAssets/The_future_of_risk/$FILE/The%20future%20of%20risk.pdf. A 2008 Ernst & Young survey of Fortune 1,000 companies indicated that the average company spends about 4 percent of revenue on risk management activities. *Id.* at 1.

[6] *Id.* at 6.

[7] An excellent discussion of scenario analysis is Elizabeth Mays, "Scenario Analysis for Board Risk Management," The Corporate Board, July/Aug. 2009.

NYSE and SEC Requirements

The New York Stock Exchange (NYSE) rules currently impose certain risk oversight obligations on the audit committee of an NYSE-listed company. Specifically, NYSE rules require that an audit committee must "discuss guidelines and policies to govern the process by which risk assessment and management is undertaken." The NYSE rules permit a company to create a separate risk oversight committee or subcommittee to perform the risk oversight function as long as the risk oversight processes conducted by that committee are reviewed in a general manner by the audit committee and the audit committee continues to discuss policies with respect to risk assessment and management.[8] Discussions should address major financial risk exposures and the steps the board has taken to monitor and control such exposure, including a general review of the company's risk management programs for non-financial matters as well. A review of the company's insurance programs to mitigate risk also would be appropriate.

Risk management is included in new proxy statement disclosures proposed by the Securities and Exchange Commission (SEC) in July 2009, scheduled to be effective for the most part in the 2010 proxy season. The proposed rules require that a company describe in its proxy statement the board of directors' role in risk management and discuss in the Compensation Discussion & Analysis section of the proxy statement the relationship between a company's overall employee compensation policies and risk management practices and/or risk-taking incentives, to the extent material.[9]

Risk Management Guidance

Boards of directors may find it useful to look to specialized organizations for guidance on the complicated business of risk management. A well-known source is the Committee of Sponsoring Organizations of the Treadway Commission (COSO), a private-sector organization sponsored by professional accounting associations and institutes, which published an enterprise risk management framework in 2004.[10] With an enterprise-wide perspective on risk management, the framework provides a useful benchmarking tool and offers detailed guidance on how a company may implement enterprise risk management procedures in its strategic planning process and through the enterprise. The COSO approach presents eight interrelated components of risk management: the internal environment (the tone of the organization), setting objectives,

---

[8] NYSE Listed Company Manual § 303A.07.

[9] SEC Release Nos. 33-9052; 34-60280; IC-28817; File No. S7-13-09 (July 10, 2009). Comments submitted with respect to the proposed rule may be accessed at http://sec.gov/comments/s7-13-09/s71309.shtml.

[10] "Enterprise Risk Management—Integrated Framework (2004)," Committee of Sponsoring Organizations of the Treadway Commission, available at http://www.coso.org/. *See also* "Effective Enterprise Risk Oversight: The Role of the Board of Directors," Committee of Sponsoring Organizations of the Treadway Commission (2009).

event identification, risk assessment, risk response, control activities, information and communications, and monitoring. Since the end of 2008, Standard & Poor's has used the COSO framework to apply enterprise risk analysis to corporate ratings, with a focus on risk-management culture and strategic risk management.[11] Moody's and Fitch also take into account risk management systems in their credit risk scoring activities.

Industries with specialized risks often require risk management guidance that is tailored to the industry. In the banking industry, regulators offer guidance as to risk management. In other industries, associations often publish guidance that is specific for the industry and may institute industry alerts to inform participants of newly identified risks and risk management procedures.

The Role of the Board

Management has the primary responsibility for risk management, and management must develop appropriate processes and procedures to identify, manage and mitigate risks. Recognizing that directors have an important role in the oversight of risk management, the board of directors should not be involved in the day-to-day activities of risk management. Directors should, instead, through their oversight role, satisfy themselves that the risk management processes designed and implemented by executives and risk managers are adapted to and integrated with the board's corporate strategy and are functioning as directed, and that necessary steps are taken to foster a culture of risk-adjusted decision-making throughout the organization. As the Center for Capital Markets Competitiveness stated recently in a comment letter to the SEC, "Corporate governance policies must promote long-term shareholder value and profitability but should not constrain reasonable risk-taking and innovation."[12] Members of the board are entitled to rely on management as well as outside advisors for their expertise in such matters. Through its oversight role, the board of directors has the ability to make clear to the company's management that corporate risk management is not an impediment to the conduct of business nor a mere supplement to a company's overall compliance program but is, instead, an integral component of the company's strategy, culture and value generation process. Through board leadership, this message can be conveyed broadly throughout the organization.

---

[11] "S&P Report on Integrating ERM Into Ratings," ComplianceWeek.com, July 28, 2009.

[12] Letter from the Center for Capital Markets Competitiveness to Ms. Elizabeth M. Murphy, Secretary, U.S. Securities and Exchange Commission, Sept. 16, 2009. The Center for Capital Markets Competitiveness is part of the U.S. Chamber of Commerce, available at http://sec.gov/comments/s7-13-09/s71309-128.pdf.