Bank and Corporate Governance Law Reporter
1601 Connecticut Avenue, N.W., Suite 701, Washington, D.C. 20009 • 202-462-5755 • Fax 202-328-2430

Risk Management and the Board of Directors

Martin Lipton, Daniel A. Neff,
Andrew R. Brownstein, Steven A. Rosenblum,
Adam O. Emmerich & Sebastian L. Fain

Wachtell, Lipton, Rosen & Katz

I. Introduction

Overview

Recent events, combined with the post-financial-crisis political and regulatory environment, have caused companies to re-assess their policies and procedures for evaluating risks and establishing risk management parameters. The risk oversight function of the board of directors continues to take center stage in this re-assessment, and investor and public expectations for board engagement with risk continue to be high. The reputational damage to boards of companies that fail to properly manage risk is a major threat.

What exactly is the proper role of the board in corporate risk management? The board cannot and should not be involved in actual day-to-day risk *management*. Directors should instead, through their risk *oversight* role, satisfy themselves that the risk management policies and procedures designed and implemented by the company's senior executives and risk managers are consistent with the company's corporate strategy and risk appetite, that these policies and procedures are functioning

Volume 45, Number 6, February 2011.

as directed, and that necessary steps are taken to foster a culture of risk-aware and risk-adjusted decision-making throughout the organization. The board should establish that the CEO and the senior executives are fully engaged in risk management. Through its oversight role, the board can send a message to the company's management and employees that comprehensive risk management is neither an impediment to the conduct of business nor a mere supplement to a firm's overall compliance program, but is instead an integral component of the firm's corporate strategy, culture and business operations.

Tone at the Top and Corporate Culture

The "tone at the top" established by the board and the CEO shapes corporate culture and permeates the corporation's internal and external relationships. The board and relevant committees should work with management to promote and actively cultivate a corporate culture and environment that understands and implements enterprise-wide risk management. Comprehensive risk management should not be viewed as a specialized corporate function, but instead should be treated as an integral component that affects how the company measures and rewards its success. Companies will, of course, need to incur risk in order to run their businesses, and there can be danger in excessive risk aversion, just as there is danger in excessive risk-taking. But the assessment of risk, the accurate calculation of risk versus reward, and the prudent mitigation of risk should be incorporated into all business decision-making. In setting the "tone at the top," transparency, consistency and communication are key: the board's vision for the corporation, including its commitment to risk oversight, ethics and intolerance of compliance failures, should be communicated effectively throughout the organization. Risk management policies and procedures and codes of conduct and ethics should be incorporated into the company's strategy and business operations, with appropriate supplementary training programs for employees and regular compliance assessments.

II. The Risk Oversight Function of the Board of Directors

A board's risk oversight responsibilities derive primarily from state law fiduciary duties, federal laws and regulations, stock exchange listing requirements, and certain established (and evolving) best practices:

State Law Fiduciary Duties – The Caremark Case–Did the Board Ignore Red Flags

The Delaware courts have developed a framework for assessing whether board oversight of risk management, in any given case, satisfies the directors' fiduciary duties. The basic rule under the *Caremark* line of cases is that directors can only be liable for a failure of board oversight where there is "sustained or systemic failure of the board to exercise oversight—such as an utter failure to attempt to assure a reasonable information and reporting system exists," noting that this is a "demanding test." *In re Caremark International Inc. Derivative Litigation*, 698 A.2d 959, 971 (Del. Ch. 1996). In cases since *Caremark*, the Delaware courts have made clear that they will not impose liability under a *Caremark* theory unless the directors intentionally failed to implement any reporting or information system or controls or, having implemented such a system, intentionally refused to monitor the system or act on warnings it provided.

Two 2009 Delaware Court of Chancery decisions have expanded upon *Caremark*, while reaffirming that the *Caremark* standard remains the fundamental standard. The plaintiffs in *In re Citigroup Inc. Shareholder Derivative Litigation* alleged that the defendants, current and former directors of Citigroup, had breached their fiduciary duties by not properly monitoring and managing the business risks that Citigroup faced from subprime mortgages and securities, and by ignoring alleged "red flags" that consisted primarily of press reports and events indicating worsening conditions in the subprime and credit markets. The Court dismissed these claims, reaffirming the "extremely high burden" plaintiffs face in bringing a claim for personal director liability for a failure to monitor business risk and that a "sustained or systemic failure" to exercise oversight is needed to establish the lack of good faith that is a necessary condition to liability.

The *Citigroup* court observed that its decision to block further litigation against the Citigroup directors could be thought to be at variance with the result in *American International Group, Inc. Consolidated Derivative Litigation*, a Delaware case decided shortly before *Citigroup*

involving shareholder claims arising out of conduct by American International Group, Inc. (AIG). In the *AIG* case, the Court of Chancery allowed claims based on alleged fraud and illegalities at AIG to survive a motion to dismiss, relying in part on a theory that the defendants had "consciously failed to monitor or oversee the company's internal controls." However, the individual defendants in the *AIG* case were executives and inside directors who were allegedly "directly knowledgeable of and involved in much of the wrongdoing," rather than independent, non-executive directors. Moreover, the *Citigroup* court relied on the distinction between business decisions and matters of corporate fraud and violations of law. Overall, the cases reflect that it is difficult to show a breach of fiduciary duty for failure to exercise oversight and that the board is not required to undertake extraordinary efforts to uncover non-compliance within the company, provided a monitoring system is in place.

In 2010, the European Commission, in a consultation paper seeking comments on options to improve corporate governance in financial institutions, suggested strengthening "legal liability of directors by an expanded duty of care." The possibility is real that higher standards of care could eventually be imposed not only on directors of financial institutions, but on directors of all corporations.

Federal Laws and Regulations

Dodd-Frank. Signed into law on July 21, 2010, the Dodd-Frank Wall Street Reform and Consumer Protection Act (the "Dodd-Frank Act") has created new federally mandated risk management procedures principally for financial institutions. The Dodd-Frank Act requires bank holding companies with total assets of $10 billion or more, and certain other nonbank financial companies as well, to have a separate risk committee which includes at least one risk management expert with experience managing risk of large companies. This requirement may be extended to bank holding companies with less than $10 billion in assets by the Federal Reserve Board.

Securities and Exchange Commission. In 2010, the SEC added requirements for proxy statement discussion of a company's board leadership structure and role in risk oversight. Companies are required to disclose in their annual reports the extent of the board's role in risk oversight, such as how the board administers its oversight function, the effect that risk oversight has on the board's process (*e.g.*, whether the persons who oversee risk management report directly to the board as whole, to a committee, such as the audit committee, or to one of the other standing committees of the board) and whether and how the board, or board committee, monitors risk.

The SEC proxy rules require a company to discuss the extent that risks arising from a company's compensation policies are reasonably likely to have a "material adverse effect" on the company. A company must further discuss how its compensation policies and practices, including that of its non-executive officers, relate to risk management and risk-taking incentives. In October 2010, the SEC proposed rules concerning the advisory votes on executive compensation arrangements mandated by the Dodd-Frank Act, including advisory votes on named executive officer compensation ("say-on-pay") and advisory votes on the frequency of the say-on-pay votes ("say-when-on-pay"). While final rules have not yet been promulgated by the SEC, the Dodd-Frank Act created a statutory requirement for say-on-pay and say-when-on-pay votes to be included in proxy statements for a company's first annual meeting occurring on or after January 21, 2011, and therefore these items will be appearing in proxy statements in the coming proxy season.

Industry-Specific Guidance and General Best Practices Manuals

Various industry-specific regulators and private organizations publish suggested best practices for board oversight of risk management. Examples include reports by the National Association of Corporate Directors (NACD)—Blue Ribbon Commission on Risk Governance and the Committee of Sponsoring Organizations of the Treadway Commission (COSO). The 2009 NACD report provides guidance on and principles for the board's risk oversight activities, the relationship between strategy and risk, the board's role in relation to particular categories of risk and ten principles for effective risk oversight. These principles include understanding key drivers of success and risks in the company's strategy, crafting the right relationship between the board and its standing committees as to risk oversight, establishing and providing appropriate resources to support risk management systems, monitoring potential risks in the company's culture

and incentive systems and developing an effective risk dialogue with management.

COSO published an integrated enterprise risk management framework in 2004 that is internationally recognized. The COSO approach presents eight interrelated components of risk management: the internal environment (the tone of the organization), setting objectives, event identification, risk assessment, risk response, control activities, information and communications, and monitoring. A COSO 2009 enterprise risk management release stresses the specific importance of the board of directors to enterprise risk management, noting that it is while it is "not a panacea," a board's involvement in risk oversight "strengthens an organization's resilience to significant risk exposures." The release recommends concrete steps for boards, such as understanding a company's risk philosophy and concurring with its risk appetite, reviewing a company's risk portfolio against that appetite, and knowing the extent to which management has established effective enterprise risk management and is appropriately responding in the face of risk.

III. Recommendations for Improving Risk Oversight

Risk management should be tailored to the specific company, but in general an effective risk management system will (1) adequately identify the material risks that the company faces in a timely manner; (2) implement appropriate risk management strategies that are responsive to the company's risk profile, business strategies, specific material risk exposures and risk tolerance thresholds; (3) integrate consideration of risk and risk management into business decision-making throughout the company; and (4) adequately transmit necessary information with respect to material risks to senior executives and, as appropriate, to the board or relevant committees.

Specific types of actions that the appropriate committees may consider as part of their risk management oversight include the following:

- review with management the categories of risk the company faces, including any risk concentrations and risk interrelationships, as well as the likelihood of occurrence, the potential impact of those risks and mitigating measures;
- review with management the company's risk appetite and risk tolerance, the ways in which risk is measured on an aggregate, company-wide basis, the setting of aggregate and individual risk limits (quantitative and qualitative, as appropriate), and the actions taken if those limits are exceeded;
- review with committees and management the board's expectations as to each group's respective responsibilities for risk oversight and management of specific risks to ensure a shared understanding as to accountabilities and roles;
- review the risk policies and procedures adopted by management, including procedures for reporting matters to the board and appropriate committees and providing updates, in order to assess whether they are appropriate and comprehensive;
- review management's implementation of its risk policies and procedures, to assess whether they are being followed and are effective;
- review with management the quality, type and format of risk-related information provided to directors;
- review the steps taken by management to ensure adequate independence of the risk management function and the processes for resolution and escalation of differences that might arise between risk management and business functions;
- review with management the design of the company's risk management functions, as well as the qualifications and background of senior risk officers and the personnel policies applicable to risk management, to assess whether they are appropriate given the company's size and scope of operations;
- review with management the means by which the company's risk management strategy is communicated to all appropriate groups within the company so that it is properly integrated into the company's enterprise-wide business strategy;
- review internal systems of formal and informal communication across divisions and control

functions to encourage the prompt and coherent flow of risk-related information within and across business units and, as needed, the prompt escalation of information to management (and to the board or board committees as appropriate); and

- review reports from management, independent auditors, internal auditors, legal counsel, regulators, stock analysts, and outside experts as considered appropriate regarding risks the company faces and the company's risk management function.

Situating the Risk Oversight Function

Most boards delegate oversight of risk management to the audit committee, which is consistent with the NYSE rule that requires the audit committee to discuss policies with respect to risk assessment and risk management. Financial companies covered by the Dodd-Frank Act must have dedicated risk management committees. The appropriateness of a dedicated risk committee at other companies will depend on the industry and specific circumstances of the company. Boards should also bear in mind that different kinds of risks may be best suited to the expertise of different committees—an advantage that may outweigh any benefit from having a single committee specialize in risk management. Regardless of the delegation of risk oversight to committees, however, the full board should satisfy itself that the activities of the various committees are coordinated and that the company has adequate risk management processes in place. To the extent risk oversight is a focus of committees, those committees should report key findings periodically to the full board and also confer amongst themselves.

If the company keeps the primary risk oversight function in the audit committee and does not establish a separate risk committee or subcommittee, the audit 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 and focus to the risk oversight role. The goal should be to achieve 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.

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. Specialized committees may be tasked with specific areas of risk exposure. Banks, for instance, often maintain credit or finance committees, while energy companies may have public policy committees largely devoted to environmental and safety issues. Where different board committees are responsible for overseeing specific risks, the work of these committees should be coordinated in a coherent manner both horizontally and vertically so that the entire board can be satisfied as to the adequacy of the risk oversight function and the company's overall risk exposures are understood, including with respect to risk interrelationships.

The board should undertake an annual review of the company's risk management system, including a review of board- and committee-level risk oversight policies and procedures, a presentation of "best practices" to the extent relevant, tailored to focus on the industry or regulatory arena in which the company operates and a review of other relevant issues such as those listed above. General reviews do not replace the need to address specific major issues when they may arise. For example, where a major risk comes to fruition, management should thoroughly investigate and report back to the full board or the relevant committees as appropriate. In order to improve the risk management procedures and to demonstrate good faith to regulators (and the media), conducting an intensive and wide-ranging review of the particular incident or condition, including interviews with managers and directors (and potentially involving outside consultants) should be considered.

Board Training and Tutorials

Understanding the material risks faced by a company and assessing the adequacy of the company's response to those risks requires an understanding of the company's underlying business. The content of orientation and training programs for new directors should be reviewed to make sure that such programs enable directors to gain an understanding of the company's business and risks.

Volume 45, Number 6, February 2011.

In addition to new director training, a company should consider the usefulness of tutorials for directors on a continuing basis, as a supplement to board and committee meetings, to help keep directors abreast of current industry and company-specific developments and issues. Offering site visits to directors, either within the framework of the board meeting schedule or as part of training or tutorials, may be valuable for some companies where physical inspection is important for appreciating the on-the-ground risks that the company faces.

Training and tutorials should be tailored to the issues most relevant and important to the particular company and its business. For example, commercial banks and investment banks that issue and deal in volatile securities and derivatives generally monitor their exposure to risk through daily calculations based on the market acting contrary to the assumptions made when the positions were established or on the previous day by means of a complex calculation of "value at risk." A tutorial as to the assumptions and the manner of calculating value at risk is important for understanding the risks the company faces. In addition, many business decisions are made in the context of the economic and political situation affecting the company, both domestically and worldwide, and a tutorial on the economic and political environment in which the company operates is useful to a director's understanding of the company's business. Outside experts may be helpful for some training, but it is not necessary to seek outside expertise, and the company's own experts may be in a better position than outsiders to explain the specific issues faced by the company. While there is no legal requirement that directors be given tutorials in order to satisfy their due care obligations, such education can be very useful. In addition, shareholder activists and regulators are increasingly pushing for this kind of continuing director education.

Board and Committee Composition

In response to corporate governance trends, companies have increased the proportion of independent directors and the diversity of those directors. In addition, active senior executives have scaled back the number of outside boards on which they serve. As a result, companies often have a number of directors who come to board service without personal, detailed knowledge of the industry in which the company operates and/or without personal experience in private sector management. This makes director training, as discussed above, all the more important. Given the challenging and complicated current risk environment, a board may also want to consider a director's background and experience in determining the composition of any committees charged with risk management oversight and with respect to the composition of the board as a whole.

When considering new director candidates, a board may want to place a greater emphasis on seeking candidates with directly relevant industry or business expertise. Where appropriate, consideration should also be given to seeking candidates with technical sophistication in risk disciplines relevant to the company and solid business experience that will provide relevant perspectives on risk issues. Where not already required under the Dodd-Frank Act, boards may wish to add a director who is a risk management expert having experience at companies in a similar industry.

Notwithstanding the governance activists' focus on independence, for a board on which the CEO is the sole management representative, consideration may also be given to adding a second or third management representative, such as the COO, CFO, or Chief Risk Officer. This may provide an additional source of direct input and information on the company's business, operations, and risk profile in the boardroom. While a company should establish direct lines of communication between non-CEO executives and the board or relevant committees in any event, actual membership on the board may be an effective means at some companies of obtaining regular, consistent and ongoing input from such executives at the board level.

Lines of Communication and Information Flow

The ability of the board or a committee to perform its oversight role is, to a large extent, dependent upon the relationship and the flow of information between the directors, senior management, and the risk managers in the company. If directors do not believe they are receiving sufficient information—including information regarding the external and internal risk environment, the specific material risk exposures affecting the company, how these risks are assessed and prioritized, risk response strategies, implementation of risk management procedures and

infrastructure, and the strength and weaknesses of the overall system—they should be proactive in asking for more. Directors should work with management to understand and agree on the types, format and frequency of risk information required by the board. High-quality, timely and credible information provides the foundation for effective responses and decision-making by the board.

Any committee charged with risk oversight should hold sessions in which it meets directly with key executives primarily responsible for risk management, just as an audit committee meets regularly with the company's internal auditors and liaises with senior management in connection with CEO and CFO certifications for each Form 10-Q and Form 10-K. In addition, senior risk managers and senior executives should understand they are empowered to inform the board or committee of extraordinary risk issues and developments that need the immediate attention of the board outside of the regular reporting procedures. In the financial institutions context, various working groups have published guidance concerning risk oversight and risk management, including with respect to risk-related committees. These groups recommend that such committees secure the attendance and participation of executives and senior leaders from key business lines, independent risk managers and control functions. An appropriate overlap of key business leaders, support leaders and enterprise executives across functions is also viewed as critical to fostering firmwide communication and cooperation. Information flow is particularly important to avoid risk of liability under *Caremark*. In particular, the board should feel comfortable that "red flags" or "yellow flags" are being reported to it so that they may be investigated if appropriate.

Legal Compliance Programs

Senior management should provide the board or committee with an appropriate review of the company's legal compliance programs and how they are designed to address the company's risk profile and detect and prevent wrongdoing. While compliance programs will need to be tailored to the specific company's needs, there are a number of principles to consider in reviewing a program. As noted earlier, there should be a strong "tone at the top" from the board and senior management emphasizing that non-compliance will not be tolerated. The compliance program should be designed by persons with relevant expertise and will typically include interactive training as well as written materials. Compliance policies should be reviewed periodically in order to assess their effectiveness and to make any necessary changes. There should be consistency in enforcing stated policies through appropriate disciplinary measures. Finally, there should be clear reporting systems in place both at the employee level and at the management level so that employees understand when and to whom they should report suspected violations and so that management understands the board's or committee's informational needs for its oversight purposes. A company may choose to appoint a chief compliance officer and/or constitute a compliance committee to administer the compliance program, including facilitating employee education and issuing periodic reminders. If there is a specific area of compliance that is critical to the company's business, the company may consider developing a separate compliance apparatus devoted to that area.

Anticipating Future Risks

The company's risk management structure should include an ongoing effort to assess and analyze the most likely areas of future risk for the company, including how the contours and interrelationships of existing risks may change and how the company's processes for anticipating future risks are developed. Anticipating future risks is a key element of avoiding or mitigating those risks before they escalate into crises. In reviewing risk management, the board or relevant committees should ask the company's executives to discuss the most likely sources of material future risks and how the company is addressing any significant potential vulnerability. Significant changes in the external environment, demographics, key relationships, technology, strategies, competitors, laws and regulations, people and processes relevant to a company may all create risks to be managed and overseen.

* * *

