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

by

Martin Lipton, Daniel A. Neff, Andrew R. Brownstein, Steven A. Rosenblum, Adam O. Emmerich, Sabastian V. Niles, & Brian M. Walker

Wachtell, Lipton, Rosen & Katz

Balancing risk and reward has never been more challenging than it is today. Companies face risks that are more complex, interconnected and potentially devastating than ever before. Over the past two years, a perfect storm of economic conditions has triggered an extraordinary downward spiral from which we are only recently beginning to emerge: the subprime meltdown, liquidity crises, extreme market volatility, controversial government bailouts, consolidations of major banking institutions and widespread economic turmoil both in the U.S. and around the world. Against the background of the global financial crisis and the still uncertain global economy, companies are re-assessing their strategies for responding to the challenges and pressures of the new environment. Risk—and in particular the risk oversight function of the board of directors—has taken center stage in this re-assessment, and expectations for board engagement with risk are at all-time highs. Risk from the financial services sector has contributed to large-scale bankruptcies, bank failures, government intervention and rapid consolidation. And the repercussions have spread to the broader economy, as companies in nearly every industry have suffered from the effects of a global constriction of the credit markets, sharply reduced consumer demand and volatile commodity prices, currencies and stock prices.

The public and political perception that undue risk-taking was central to the breakdown of the financial and credit markets has fueled an extensive legislative, regulatory, and even judicial focus on risk management and risk prevention. A number of legislative and regulatory proposals that address or touch upon risk-related items are currently pending. The Securities and Exchange Commission recently proposed disclosure rules that would require discussion in proxy statements of the board's role in overseeing and managing risk and the relationship between a company' s overall employee compensation policies and risk management. Bills introduced in Congress have called for independent risk committees responsible for the establishment and evaluation of risk management practices to be formed at large financial institutions as well as other publicly listed companies. Risk management is also likely to receive heightened focus by shareholder activists and other "good governance" proponents, and the SEC has recently liberalized its approach to shareholder proxy proposals addressing risk oversight. While we expect that the business judgment rule will survive the financial crisis intact, boards and companies should remain mindful in the current environment of the possibility that courts may apply new standards, or interpret existing standards, to increase board responsibility for risk management. Finally, the reputational damage to companies and boards of flawed risk management processes must also be considered.

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 processes designed and implemented by the company's risk managers are consistent with the company's corporate strategy and are functioning as directed, and that necessary steps are taken to foster a culture of risk-aware and risk-adjusted decision-making throughout the organization. Establishing the right "tone at the top" of the corporation is one of the most important factors in

Volume 43, Number 6, February 2010.

ensuring that a board functions effectively and is able to meet all of its responsibilities, particularly with respect to risk oversight. Through its oversight role, the board can send a message to the company's management and employees that comprehensive corporate 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 value-generation process. Much has been said on the need for boards to find the right balance between monitoring compliance and advising on strategy. In the arena of risk oversight, these dual roles of monitor and strategic advisor converge.

A company's risk management system should function to bring to the board's attention the company's most material risks and permit the board to understand and evaluate how those risks interrelate, how they affect the company, and how management addresses those risks. Given the challenges and complexities of the current risk environment, companies may want to refocus on industry experience and qualifications in their new director selection process, and, in addition, provide tutorials to help their directors better understand and assess the risks the company faces. Proposed revisions to proxy statement disclosure obligations would expand required information about directors and director nominees, mandating a discussion of the specific experience and skills relevant to service as a director and, where applicable, as a committee member.

The board should also consider the best organizational structure to give risk oversight sufficient attention at the board level. In some companies, this may include creating a separate risk management committee or subcommittee. In others, it may be most effective to schedule the review of risk management as a dedicated and periodic agenda item for an existing committee such as the audit committee, coupled with periodic review at the full board level. Risk management can also be allocated among existing committees as long as the committees coordinate their risk management efforts and share information appropriately with each other and with the full board. While no "one size fits all," it is important that risk management be a priority and that a system for risk oversight appropriate to the company be in place.

This memorandum outlines the risk oversight obligations of the board of directors and certain best practices derived from governmental, regulatory and other sources and provides recommendations for structuring and improving risk oversight at the board level. Attached as Appendix A to this memorandum is a discussion of some of the common areas of risk that companies may face.

The Risk Oversight Function of the Board of Directors

A board's risk oversight responsibility derives 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 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 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 was 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 there would be no liability under a *Caremark* theory unless the directors intentionally failed entirely 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.

The February 2009 Delaware Court of Chancery decision in *In Re Citigroup Inc. Shareholder Derivative Litigation* demonstrates that the *Caremark* standard remains intact, even in the current environment. The plaintiffs in the case 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. Declaring that "oversight duties under Delaware law are not designed to subject

directors, even expert directors, to personal liability for failure to predict the future and to properly evaluate business risk," the Court dismissed these claims. In doing so, the Court reaffirmed 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 decision also drew an important distinction between oversight liability with respect to business risks and oversight liability with respect to illegal conduct, emphasizing that Delaware courts will not permit "attempts to hold director defendants personally liable for making (or allowing to be made) business decisions that, in hindsight, turned out poorly." Bad business decisions are not evidence of bad faith.

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 another recent Delaware case 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 (some of whom were AIG directors) 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 noncompliance within the company, provided a monitoring system is in place. In light of the ongoing political and legislative focus on risk oversight, however, boards should recognize the possibility that what constitutes a "red flag" and what constitutes conscious disregard may be evaluated in the future with heightened scrutiny. Moreover, it is important to note that the courts have taken the view that if a breach of duty for failure to exercise oversight is found, directors are not protected by corporate exculpation or indemnification provisions.

To avoid risk of *Caremark* liability, boards should ensure that the company implements appropriate reporting and monitoring systems tailored to each type of material risk applicable to the company. The board should periodically review these monitoring systems and ask management and/or outside consultants for an assessment of the systems' adequacy. The board should be sensitive to "red flags" or "yellow flags," causing them to be investigated if appropriate, and should document these activities in minutes or other documents that accurately convey the time and effort spent by the board and its advisors. With respect to compliance matters, the monitoring system should include reports on material regulatory proceedings, or material regulatory fines or censures. The board should treat material regulatory proceedings as worthy of board monitoring.

Federal Laws and Regulations

Federal legislation and regulations often address risk management issues. In addition, companies with business operations in countries outside the U.S. should be aware of legal requirements in each such jurisdiction. Whether or not a direct obligation relating to risk management is imposed on the board, such laws and regulations will influence the risk management activities that a company should undertake. In the context of the current environment and focus on risk management and risk oversight, a failure by the board to oversee a system of compliance with material legal requirements may not only raise issues under state fiduciary duty standards, but, depending on the type of legal requirement at issue, may also give rise to other claims such as tort liability or even criminal liability. Thus, the board should be made aware of material legal requirements applicable to the company, and seek assurance that the company has taken these requirements into account in constructing its risk management system.

Proposed Legislation

In response to the financial crisis, Congress and federal agencies have proposed new legislation regarding risk management disclosure and oversight. Much of this proposed legislation focuses

on the intersection between risk management and compensation practices. While financial institutions have been the focus of many of the proposals, the importance of aligning risk exposures with the company's appropriate risk tolerance and the relationship between risk-taking and compensation has implications for nonfinancial companies as well. In May 2009, Senator Charles Schumer introduced the so-called "Shareholder Bill of Rights Act of 2009" which, among other things, would require all public companies to create separate risk committees responsible for the establishment and evaluation of risk management practices and comprised entirely of independent directors. The bill has been criticized for its "one size fits all" approach to risk management and its potential to exacerbate the problem of balkanization and fragmentation in the boardroom. Similarly, legislation proposed by Senator Christopher Dodd would require covered financial institutions to establish such a committee for supervising enterprise-wide risk management practices. The committee would include independent directors and, significantly, at least one risk management expert having experience in identifying, assessing, and managing risk exposures. It is not yet clear whether these proposals will eventually be enacted.

Securities and Exchange Commission

In July 2009, the SEC proposed rules that would require companies to provide greater disclosures about their risk oversight practices, including information as to the board's role in risk management. The relationship between a company's overall compensation policies and its risk profile would also need to be disclosed, as would additional information concerning the qualifications and experiences of directors and director nominees. In addition, the SEC has made policy changes to facilitate the ability of shareholders to submit shareholder proxy proposals relating to risk oversight and management. This reflects the SEC's conclusion 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."

Executive Compensation and Risk-Taking

Concern that compensation arrangements have encouraged excessive risk-taking has led to a battery of sweeping legislative and regulatory responses that would regulate executive compensation and company-wide compensation policies and impose heightened disclosure obligations. Recommendations included in the Declaration of the Summit on Financial Markets and the World Economy, issued by the White House on November 15, 2008, state that "Financial institutions should have clear internal incentives to promote stability, and action needs to be taken, through voluntary effort or regulatory action, to avoid compensation schemes which reward excessive short-term returns or risk-taking." In June 2009, Treasury Secretary Timothy Geithner indicated that in the Obama Administration's view, the financial crisis was attributable in part to "[i]ncentives for short-term gains [that] overwhelmed the checks and balances meant to mitigate against the risk of excess leverage." Accordingly, Secretary Geithner called for improved alignment between compensation paid to executives and the long-term risks borne by the company. He also advocated increased transparency around risk management and strengthened authority for risk managers to improve their effectiveness.

While the spotlight on compensation initially fell most heavily on financial institutions, given the uncertainty engendered by this barrage of congressional and regulatory proposals, financial and non-financial companies alike should review their compensation plans and programs in the context of risk management and risk oversight with a view to whether the compensation structure encourages excessive risk-taking. To the extent that compensation is viewed publicly or politically as creating incentives to take on inappropriate risks, the interaction between compensation and risk will inevitably find its way into other legislative and regulatory responses and/or become a focus of shareholder activism and media attention. "Say-on-pay" rules and legislation requiring shareholder advisory votes on executive compensation will put additional spotlight on compensation practices.

Sarbanes-Oxley

The Sarbanes-Oxley Act of 2002 imposes numerous requirements on companies and boards, including audit committee oversight of auditors, CEO/CFO certification of quarterly and annual financial statements and reports, maintenance of internal financial controls and disclosure controls, enhanced disclosure of non-GAAP financial measures in public disclosures, and a ban on personal

loans to directors and officers. While not directly tied to risk oversight, compliance with Sarbanes-Oxley obligations should take into account risk management issues as well. For example, in determining the effectiveness of financial controls, or in the certification process for financial statements, the company should focus on whether material risks are identified and disclosed as part of the process. In reviewing the company's compliance with Sarbanes Oxley obligations, the board should inquire as to whether these risk management issues have been taken into account.

Federal Sentencing Guidelines

Under the federal sentencing guidelines relating to corporate criminal liability, a company may, under some circumstances, receive more lenient punishment if it has in place an effective compliance and ethics program. For such a program to qualify, the company must exercise due diligence and establish standards and procedures to prevent and detect criminal conduct and "otherwise promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law." In addition, the board must know about the content and operation of the program and exercise oversight with respect to its implementation and effectiveness. Given that non-compliance with law may be a key risk area for a company, this kind of compliance and ethics program should be integrated with the company's risk management program and reviewed as part of board and committee oversight of risk management.

Other Laws and Regulations

Compliance with laws and regulations as a general matter should be part of an effective risk management system. A number of the material risks outlined in Appendix A, including fraudulent conduct by employees, foreign corrupt practices, products liability, health and safety, environmental compliance, data security, customer privacy, employment practices, and antitrust compliance, are governed by various legal requirements. Again, the role of the board is not to manage compliance with these requirements on a day-to-day basis, but to be comfortable that the company has a system to address these compliance issues adequately and to bring to the board's attention material problems and risks that may arise in connection with this compliance.

Stock Exchange Rules

New York Stock Exchange rules impose certain risk oversight obligations on the audit committee of a listed company. Specifically, while acknowledging that "it is the job of the CEO and senior management to assess and manage the listed company's exposure to risk," NYSE rules require that an audit committee "discuss guidelines and policies to govern the process by which risk assessment and management is undertaken." 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. The NYSE rules permit a company to create a separate committee or subcommittee to be charged with the primary risk oversight function as long as the risk oversight processes conducted by that separate committee or subcommittee 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.

Industry-Specific Guidance and General Best Practices Manuals

Boards may also derive guidance on their risk oversight role from various industry-specific regulators and private organizations that publish suggested best practices. Examples of these include:

National Association of Corporate Directors— Blue Ribbon Commission on Risk Governance

In October 2009, the NACD published a report that 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 for the business and associated 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. Categories of risks include

governance risks, critical enterprise risks, board approval risks, business management risks and emerging and nontraditional risks.

Committee of Sponsoring Organizations of the Treadway Commission

COSO, a private-sector organization sponsored by professional accounting associations and institutes, published an integrated enterprise risk management framework in 2004 that is now internationally recognized. Promoting an enterprise-wide perspective on risk management, the framework provides a benchmarking tool and offers detailed guidance on how a company may apply and implement enterprise risk management procedures in its strategic planning and across the entire organization. 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. COSO periodically releases guidance to supplement the framework and assist companies in shaping conforming procedures. A COSO 2009 enterprise risk management release stresses the specific importance of the board of directors to enterprise risk management and the need for the board to understand and shape the organization's risk appetite, risk philosophy and risk portfolio and to assure that risk management mechanisms are aligned and effective.

Banking Industry

In the highly regulated banking industry, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation and the Office of the Comptroller of the Currency routinely publish circulars, handbooks, manuals and other materials prescribing effective risk management frameworks for banks and providing guidance to boards of banks with respect to specific risks faced by banking institutions. These regulators also provide direct guidance to boards on their risk management policies and effectiveness vis-à-vis specific banking regulations during periodic reviews. As in any regulated industry, it is important for regulated financial institutions to understand the principal general risk areas being identified from time to time by regulators through supervisory letters, speeches, enforcement or supervisory actions involving peer institutions and the like, and to understand how their institutions are positioned with respect to such risks. At many financial institutions, regulators work with company personnel on a daily basis, and the board should satisfy itself that there is an adequate procedure in place to promptly alert senior management to problems or tensions that develop in that relationship.

Other Industry-Specific Guidelines

Various industry groups and specialized risk management organizations have produced manuals and guidelines outlining best practices for managing risks specific to certain industries such as utilities, ports, nuclear materials management and pharmaceuticals. Such guidance addresses the specific risk environment in the respective industry and provides recommendations on risk management procedures and best practices that boards and senior managers in these industries should consider when designing and implementing risk management programs.

Reputational Issues

The threat of reputational damage from lack of adequate risk oversight provides an overlay to the specific risk management-related laws, regulations, stock exchange rules and best practice manuals. Apart from the question of legal exposure, the board of a company whose excessive risk-taking leads to a crisis or poor results will face criticism in the press, in the political arena, and from shareholder activists. Under these circumstances, the board may also face proxy contests, either from a competing slate or through withhold authority campaigns. For example, Change to Win Investment Group has engaged in proxy attacks against directors that it views as responsible for failures of risk oversight, initially focusing on the banking industry. The business press and other activist groups also highlight and target directors that they view as underperforming. With the current focus on risk oversight and management, one can expect that these "lists of shame" will include a focus on companies perceived to have taken on excessive levels of risk.

Recommendations for Improving Risk Oversight

In fulfilling its risk oversight role, the board should focus on the adequacy of the company's risk management process and overall risk management

system. 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 and specific material risk exposures; (3) integrate consideration of risk and risk management into business decision-making throughout the company; and (4) include policies and procedures that adequately transmit necessary information with respect to material risks to senior executives and, as appropriate, to the board or relevant committees.

The following sets forth recommendations that may help the board in carrying out its risk oversight role:

Tone at the Top and Corporate Culture

Of critical importance in effective risk oversight and day-to-day risk management is having the right "tone at the top" of the corporation. The "tone at the top" 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 enterprise-wide risk management, incorporates it into overall corporate strategy and day-to-day business operations and gives high priority to riskaware and risk-adjusted decision-making. Comprehensive risk management should not be viewed as hindering corporate progress, or isolated 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 set out in the annual report and 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 operations, with appropriate supplementary training programs for employees and regular compliance assessments.

Risk Oversight Roles of the Board and its Committees

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. For some companies, the scope and complexity of risk management may make it desirable to create a dedicated risk management committee or subcommittee to permit greater focus at the board level on risk management and oversight. The appropriateness of a dedicated risk committee often depends on the industry and specific circumstances of the company. Boards should bear in mind that different kinds of risks may be best suited to the expertise of different committees—an advantage that often outweighs any benefit from having a single committee specialize in risk management. The NYSE rule permits boards to delegate the primary risk oversight function to a separate board committee, subject to limited continuing audit committee oversight. 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 one or more committees, those committees should report key findings periodically to the full board.

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 specifically. 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. For example, the company's compensation structure may benefit from review to avoid incentives that promote excessive risk-taking. Moreover, specialized committees may be tasked with specific areas of risk exposure. Banks, for instance, often maintain credit or finance committees, while some energy companies 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 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.

Risk Oversight Activities

In overseeing risk management, the types of actions that the board and appropriate committees may consider taking include the following:

- review with management the company's risk appetite and risk tolerance, the ways in which risk is measured on an aggregate, company-wide basis, and the setting of aggregate and individual risk limits (quantitative and qualitative, as appropriate) and the actions taken if those limits are exceeded;
- 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 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, 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, including as to potential coverage gaps and reporting lines of authority, 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 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.

Similarly, the COSO enterprise risk management framework highlights several key areas that may contribute to effective board risk oversight, including understanding and shaping the company' s risk philosophy, concurring with the company's risk tolerance, knowing the extent to which management has established enterprise risk management programs at the company, reviewing the company's portfolio of risk and considering it against the risk

tolerance, staying apprised of the most significant risks, and assessing the appropriateness of management's response to risk exposures.

The board may also consider scheduling 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. Regularly scheduled reviews do not replace the need to address specific major issues when they may arise. For example, where a major risk comes to fruition (*e.g.*, a serious accident), management should thoroughly investigate the incident and report back to the full board or the relevant committees as appropriate. In order to reduce the likelihood of losses 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 quickly, and the company's risk profile should be incorporated into that training. If necessary, additional time and content should be devoted to educating new directors so that they have a full picture of the company.

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 specialized 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. For example, where applicable, a visit to a factory, offshore oil rig, mine, pharmaceutical lab, or other relevant site may allow directors to assess firsthand some of the health and safety, operational and other risks facing the company better than a report or written description.

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 such a company is facing, particularly in light of the current financial and economic environment. In addition, many business decisions are made in the context of the economic and political situation affecting the company, 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 are often 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 made great strides in increasing the independence and diversity of their boards. In addition, active senior executives have scaled back the number of outside boards on which they serve. One result of these trends, however, is that 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, to the extent such expertise is not already well represented on the board. 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.

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, to 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, 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 effectively 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 10-Q and 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 firm-wide communication and cooperation.

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 any program. 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 a clear reporting system in place so that employees understand when and to whom they should report suspected violations. 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. Anticipating future risks is obviously 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, people and processes relevant to a company all create risks to be managed and overseen.

