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, Shaun J. Mathew, Brian M. Walker, & Philipp von Bismark

Wachtell, Lipton, Rosen & Katz

I. Introduction

The risk oversight function of the board of directors has never been more critical and challenging than it is today. In the context of the current global financial crisis and the swooning global economy, companies now face risks that are more complex, interconnected and potentially devastating than ever before. 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 paralysis in the credit markets, sharply reduced consumer demand and extremely volatile commodity, currency and stock markets. In addition, the public and political perception that undue risk-taking has been central to the breakdown of the financial and credit markets is leading to an increased legislative and regulatory focus on risk management and risk prevention. In this environment, boards and companies must be mindful of the possibility that courts will apply new standards, or interpret existing standards, to increase board responsibility for risk management.

But 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 executives and risk managers are adapted to 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. Through its oversight role, the board can send a message to the company's management and employees that corporate risk management is not 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.

Given the increased significance of the risk oversight role in the current risk environment, 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 these risks interrelate, how they affect the company, and how management addresses these risks. It is important for directors to have the experience, training and knowledge of the business necessary for making a meaningful assessment of the risks that the company faces, however complicated they may be. 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 sufficient to have the review of risk management as a dedicated, periodic agenda item for an existing committee such as the audit committee, in addition to periodic review at the full board level. 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 put in place.

This memorandum (1) outlines the risk oversight obligations of the board of directors and certain best practices derived from governmental and regulatory sources, (2) discusses some of the common areas of risk that companies may face, and (3)

Volume 42, Number 2, April 2009.

provides recommendations for structuring and improving risk oversight at the board level.

II. The Risk Oversight Function of the Board of Directors

A board's risk oversight responsibility derives primarily from state law fiduciary duties, U.S. and foreign laws and regulations, stock exchange listing requirements, and certain established best practices. In addition, the threat of reputational damage from shareholder activism or adverse media attention for companies perceived to have poor risk management also plays a role in determining the proper risk oversight behavior of corporate boards. We discuss each of these below.

State Law Fiduciary Duties

The Delaware courts have developed a framework for the board oversight of risk management in a line of cases dealing with alleged violations of fiduciary duty. In the first of these cases, the Delaware Chancery Court stated that director liability for a failure of board oversight required a "sustained or systemic failure of the board to exercise oversight – such as an utter failure 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). The cases that followed 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 any warnings it provided.

In recent years, the few *Caremark* claims to survive motions to dismiss have involved an absence of any monitoring system or clearly egregious behavior. For instance, in one case, a court found the company's directors liable for failure to monitor because no system was in place to supervise or control the making of multimillion dollar loans to corporate insiders. In another case, a court held that the company's directors had consciously ignored red flags indicating a systemic scheme of criminal Medicare fraud. In light of the widespread nature of the fraud, the fact and scope of ongoing government investigations, the health care expertise of the board members and an extended investigation by *The New York Times*, the court found that the board's failure to act on these red flags constituted intentional or reckless disregard.

These cases demonstrate that it is difficult to show a breach of fiduciary duty for failure to exercise oversight; these cases do not require the board to undertake extraordinary efforts to uncover non-compliance within the company. In light of the focus on risk oversight in the current environment, 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 focus. Moreover, it is important to note that the courts have taken the view that a breach of duty for failure to exercise oversight would be a breach of the duty of loyalty, which is not subject to exculpation or indemnification by the company. Accordingly, a board is best advised to act well above the minimal standards established by *Caremark* and its progeny.

To avoid risk of *Caremark* liability, boards should ensure that the company implements appropriate monitoring systems tailored to each type of risk. The board should periodically review these monitoring systems and ask management and/or outside consultants for an assessment of the systems' adequacy. Directors should also involve the company's general counsel as appropriate with respect to fulfilling the board's duty to have effective monitoring systems. The board should be sensitive to "red flags" or "yellow flags," investigating them or causing them to be investigated as necessary, and should document its monitoring and investigatory activities in minutes that accurately convey the time and effort spent by the board. The monitoring system should include reports on material regulatory proceedings, or material regulatory fines or censures, that may be used by plaintiffs to allege knowledge of non-compliance. The board should treat material proceedings of this kind as a red flag and investigate appropriately.

U.S. and Foreign Laws and Regulations

In recent years, risk management issues have found their way into federal legislation and regulations. In addition, companies with business operations in other countries should be aware of legal requirements in each of those jurisdictions. 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 may decide to 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 may also give rise, depending on the type of legal requirement at issue, 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 the company should take these requirements into account in constructing its risk management system.

Emergency Economic Stabilization Act of 2008. The most recent example of legislation with provisions focused on risk management is the Troubled Asset Relief Program (TARP) contained in the recently passed Emergency Economic Stabilization Act of 2008. Under this Act, the U.S. Department of the Treasury requires that boards of companies participating in the TARP Capital Purchase Program (CPP) abide by certain executive compensation standards that relate to corporate risk-taking, including "ensuring that incentive compensation for senior executives does not encourage unnecessary and excessive risks that threaten the value of the financial institution."

In connection with this requirement, Treasury's interim rules provide that the compensation committee of a company participating in CPP must take three steps: First, shortly after the company's sale of securities to Treasury, the company's compensation committee must meet with the company's senior risk officers to review each senior executive's incentive compensation arrangements and verify that the arrangements do not encourage the senior executive to take risks that would threaten the value of the company. Second, the compensation committee and senior risk officers must have an annual meeting to discuss whether and how each senior executive's incentive compensation arrangements comply with the company's risk management policies and procedures. In both the initial and annual meetings, the compensation committee and senior risk officers must identify and limit any features of the senior executive's incentive compensation arrangements that could encourage unnecessary or excessive risks. Third, the compensation committee must certify that it has completed these reviews and that it has made reasonable efforts to assure that senior executive incentive compensation arrangements do not encourage unnecessary or excessive risks. A public company must include this certification in the Compensation Discussion and Analysis of its annual proxy statement. A non-public company must provide this certification to its primary regulator.

While these requirements, by their terms, apply only to companies participating in the CPP, they evidence a concern at the federal legislative level with the issue of how compensation programs may drive risk-taking. For this reason, companies that are not subject to the CPP requirements should still consider reviewing 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 a key source of inappropriate risk, 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. For example, one of the recommendations included in the Declaration of the Summit on Financial Markets and the World Economy, issued by the White House on November 15, 2008 following the initial meeting of the Group of Twenty, states 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."

It is also worth noting that several financial supervisory authorities, lawmakers and private institutions in the EU have recently adopted measures aimed at remuneration policies that may create incentives for risk-taking that are inconsistent with sound risk management. These measures were taken in response to remuneration policies implemented at many companies that governmental authorities, economic experts and media representatives labeled inappropriate and viewed as providing incentives to management to pursue risky policies that undermined systems designed to control risk, thereby contributing to the present financial market crisis. The United Kingdom, France and Italy have taken first steps towards implementing new rules

to address these concerns, and lawmakers in other countries, such as Germany, are preparing statutory regulations which have yet to obtain parliamentary approval.

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 periodic reports, maintenance of 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. 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 federal sentencing guidelines relating to corporate criminal liability, a company may, under some circumstances, receive a more lenient sentence if it has in place an effective compliance and ethics program. In order for a program to qualify as an effective compliance and ethics program, 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 any company, this kind of compliance and ethics program may be integrated as part of 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 material risks outlined in the next section of this memo, 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 have a system that gives the board comfort that these compliance issues are being addressed within the company and that material problems and risks that may arise in connection with this compliance are brought to the board's attention.

Legislation and regulation in some foreign jurisdictions have become increasingly aggressive in imposing liability for a failure to exercise adequate care in various aspects of a company's business operations. For example, in 2007 the United Kingdom enacted the Corporate Manslaughter and Corporate Homicide Act. This Act imposes criminal liability on a company operating in the U.K., whether it is incorporated in the U.K. or abroad, if the way in which company activities are managed or organized results in a person's death and amounts to a gross breach of a duty of care by senior management. Relevant duties of care owed by a company exist, for example, in respect of the systems of work and equipment used by employees or contractors, the condition of worksites and other premises occupied by the company, and products and services supplied to customers. Notably, juries are also charged with considering whether any attitudes, policies, systems or accepted practices within the organization were likely to have encouraged or produced tolerance of any failure to comply with health and safety legislation related to the breach of the duty of care. While the Act only imposes company-level liability and specifically excludes individuals from its ambit, individuals (including directors) may still be prosecuted under existing laws for gross negligence, manslaughter, culpable homicide and for health and safety offenses.

Stock Exchange Rules

New York Stock Exchange (NYSE) rules 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." 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.

However, the 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 specialized risk management organizations that publish suggested best practices. Examples of these include:

Committee of Sponsoring Organizations of the Treadway Commission. The Committee of Sponsoring Organizations of the Treadway Commission (COSO), a private-sector organization sponsored by professional accounting associations and institutes, published an enterprise risk management framework in 2004. 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. The COSO enterprise risk management framework has become well accepted. S&P uses the framework's principles for evaluating financial companies for purposes of its ratings analysis and intends to begin using these principles when rating companies in other industries as well. Moody's and Fitch also take into account risk management systems in their credit risk scoring activities.

Banking Industry. In the highly regulated banking industry, the Office of the Comptroller of the Currency, the Federal Reserve Board, and the Federal Deposit Insurance Corporation routinely publish circulars, handbooks and manuals 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.

Other Industry-Specific Guidelines. Various industry groups and specialized risk management organizations have produced manuals or 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.

Foreign Jurisdictions. In foreign jurisdictions such as the United Kingdom, France and Germany, corporate governance codes help guide the board's role in defining and overseeing the risk management programs of public companies. The corporate governance guidelines for public companies in the U.K., for example, are set forth in the Combined Code on Corporate Governance and certain complementary reports, including the Turnbull Report, that contain detailed guidance on how risk management and internal control systems should be set up and operated. Under the Combined Code, the board's role is to provide entrepreneurial leadership of the company within a framework of prudent and effective controls that enable risk to be assessed and managed. In implementing the obligation to "safeguard shareholders' investment and the company's assets" by maintaining a sound system of internal controls, boards are expected to review, at least annually, all material controls, including risk management systems. The Turnbull Report expands upon the importance of a risk-based approach to internal controls and provides detailed guidance on establishing and reviewing appropriate risk management processes, including with respect to assessing how significant risks have been identified, evaluated and managed and determining whether any remedial ac-

tion is necessary or revisions should be made to the system.

The Financial Reporting Council, an independent regulator, undertakes regular reviews of the impact and implementation of the Combined Code and the Turnbull Report. Unlike Sarbanes-Oxley, the Combined Code is not a rigid and enforceable set of rules, but rather a guide to the components of good board practice, with respect to which U.K. law follows a "comply or explain" approach. A listed company may choose not to comply with one or more provisions of the Combined Code, but must in such cases give shareholders a "careful and clear explanation" illustrating how its actual practices contribute to good governance and are consistent with the principle to which the particular provision relates. The degree of compliance or non-compliance with the Combined Code generally plays an important role in how investors and the media judge the quality of company management.

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.

III. Some Common Areas of Risk

The following is a non-exhaustive list of some of the risks commonly faced by many major companies and business enterprises. The general advice remains the same for all types of risk: while it is not the role of the board or its designated committee to directly manage and specifically address each of the risks the company faces, the members of the board or the relevant committee should be aware of the relevant risks and satisfy themselves that management (1) designs and implements risk management policies and infrastructure that sufficiently address the relevant risk issues, (2) ensures the effectiveness of the risk policies and infrastructure, and (3) reports on these issues to the board or the committee.

Beyond the specific legal framework associated with each of these areas of risk, the company and the board should keep in mind the threat of reputational damage associated with these risks. A company's brand image and reputation can directly impact its profitability, sales, stock price and a variety of other important strategic areas. Reputation and image can be materially harmed by negative attention in the media, publicity stemming from adverse litigation, shareholder activism, protests and boycotts by special interest groups, and the general threat of customer dissatisfaction, all of which may ensue from a failure to oversee and manage risks properly.

Not every risk, of course, will be relevant to every company, and the significance of various risks will also vary from company to company. Accordingly, risk identification is an important starting point for construction of a comprehensive risk management and risk oversight system. Senior executives should devote time and attention to considering the most significant risks that face their company and educate the board or appropriate committee with respect to these risks in the context of periodic reviews of the company's risk management structure.

Financial Risks

The global financial crisis has confirmed the importance and danger of financial risks. The banking and financial services industries, of course, have been hard hit by investments in risky financial instruments, including sub-prime loans, mortgage-backed securities and structured investment vehicles. The risks associated with these investments have received much attention and press. Companies in these industries are highly focused on trying to sort through the damage inflicted by these investments and developing systems for managing and

monitoring financial risks more effectively going forward.

Companies in other industries may also face a variety of financial risks and, to the extent they are material to the company, it is important for such companies, and their boards, to understand and manage these risks as well. For example, a company should be attentive to liquidity needs and risks and consider appropriate stress testing procedures to measure the effects of potential liquidity shocks both from operations and from disruptions in the financial markets. To the extent a company engages in hedging activity, whether in connection with supply inputs (*e.g.*, oil or other commodities), foreign currency exchange or otherwise, the risk management system should consider the risks associated with that activity. This may include counterparty risks (*e.g.*, risk that a counterparty may not be creditworthy) and operational risks, such as the risk that documentation inaccurately reflects business deals and thus could lead to ineffective hedging or unintended exposures. Given the complexity of some of these financial risks and instruments, where a company's exposure is significant, the board should consider asking for periodic reports and tutorials by management and, if necessary, outside consultants.

Fraud

The increasing complexity of global companies, markets, underlying business transactions, financing structures, and financial reporting processes, together with the pervasiveness of ever-more-sophisticated information technologies, has widened opportunities for fraud and other unethical behavior, such as theft, bribery, corruption, or accounts manipulation, in many areas and from varied sources, including executives, employees, and third parties. At the same time, the potential adverse implications and consequences of fraud have reached new levels. A company with an employee or employees involved in fraudulent activities may face immediate monetary damages, other legal consequences, and damage to the company's reputation. In the longer term, the company may also encounter greater scrutiny by regulatory authorities, the media, investors, customers and the broader public. In extreme cases, fraudulent activity may lead to losing necessary licenses and the inability to continue conducting business.

The number of corporate scandals in recent years involving large, global companies has illustrated anew the need for sound risk management programs and robust internal oversight with respect to corporate fraud and unethical behavior. These include the recent losses by French banks Société Générale, Caisse d'Epargne, and Crédit Agricole of €4.9 billion, €751 million, and €250 million, respectively, due to unauthorized proprietary trading by the banks' trading personnel; large-scale accounting manipulation at companies such as Enron, WorldCom and Parmalat S.p.A.; and the widespread backdating of stock option grants.

It is important for the board and senior management to set the appropriate "tone at the top" with respect to the company's attitude toward corporate fraud and unethical behavior. Increasingly, companies have codified specific guidelines, such as anti-fraud policies (which may be a subset of the company's code of conduct, code of ethics, or governance code). Such policies should be made known throughout the company, and employees should be made aware of fraud-related risks. The board should also ask the company to maintain appropriate monitoring and auditing processes as well as effective mechanisms for reporting suspected misconduct, such as through line management or anonymous whistle-blowing hotlines and other appropriate fraud control reporting systems.

Bribery/Foreign Corruption

If a company is engaged in business activities abroad, attention should be given to risks arising from potential violations of the Foreign Corrupt Practices Act (FCPA) and similar applicable regulations. U.S. federal prosecutors have been expanding their enforcement of laws prohibiting bribery of foreign officials against both U.S. and non-U.S.-based companies. Several prominent multinational companies have faced allegations of serious violations of the FCPA or similar domestic or international anti-bribery regulations. Where applicable, a board should discuss the company's FCPA compliance program as part of its risk oversight role. Emerging best practices include (1) designating a senior officer with relevant expertise to manage the program, (2) establishing anonymous reporting mechanisms, (3) implementing internal controls to ensure that all potentially sensitive payments are approved in advance, (4) conducting due diligence

on the firm's local agents and partners, and (5) regularly auditing the business lines most likely to encounter FCPA-related issues. Due diligence with respect to FCPA-related risks – and understanding the U.S. Department of Justice's guidance for minimizing the risk of inheriting FCPA liability – is also important when acquiring a company with foreign business activities.

Disasters

Companies should attempt to model and prepare crisis management procedures for the potential occurrence of material disruptions in the financial system, terrorist attacks, natural disasters such as earthquakes or tsunamis, weather extremes like hurricanes or floods, or company-specific disasters such as industrial accidents. A company can take a variety of preventive measures to respond to particular risks and the consequences arising therefrom. For example, firms with facilities in areas that are vulnerable to seismic activity or regular floods may wish – or be legally compelled – to build or retrofit in anticipation of an earthquake or a flood. Insurance coverage and a variety of catastrophe-linked securities are also available to companies seeking to protect the value of their physical assets.

Beyond measures addressing specific aspects of the anticipated risk scenario, companies should consider comprehensive disaster planning to allow the firm to react immediately to and cope with an emergency situation, to mitigate direct and indirect consequences of the crisis, and to maintain business continuity. Disaster planning may address many aspects of a response, including emergency procedures to evacuate people and important assets, special responsibilities for crisis management, availability of alternate sites, information and communication technology and other necessary infrastructure, alternate supply chain scenarios, emergency staff planning, emergency liquidity planning, communication strategies, product callback, exchange procedures, and the like.

Products Liability

Products liability risks arise both from the risk of large-scale damage awards through jury verdicts or settlements in products liability lawsuits and from increasingly strict product safety laws and regulations (violations of which may also be used against a company in a private lawsuit). An example of recent legislation in this area is the Consumer Product Safety Modernization Act, enacted in August 2008 in response to consumer product safety issues in connection with a large number of recalls of imported goods which contained ingredients deemed to be hazardous, including children's toys, seafood, pet food, tires, and other products imported from China and other countries. Besides implementing stricter rules for children's products, this Act also expands the authority of the Consumer Product Safety Authority to request recalls of defective products from manufacturers, distributors, importers and retailers and increases the maximum penalty for violations to $15 million.

In addition, many foreign countries have introduced or significantly tightened their respective products liability regulations, posing further sources of risk for U.S. manufacturers, product sellers, or service providers doing business abroad to be sued or subjected to government regulatory action under such regulations. This is particularly true for the member states of the EU, as well as for many Asian jurisdictions such as China, Hong Kong, Japan, India, Australia, and South Korea, all of which have adopted some form of products liability act. Together with regulatory action in many of these countries, there has been a significant rise in consumer awareness of legal rights in connection with defective products and also in the level of public and media attention to product safety issues. Accordingly, products liability claims have increased in many of these countries.

A comprehensive program to manage products liability risks should include all relevant business functions of the company, from engineering, procurement, manufacturing and quality control to sales and distribution. Specific measures should be taken by companies that outsource the engineering and/or manufacturing of products, including obtaining approval rights over subcontractors and suppliers and control rights over outsourcing by approved suppliers. This may be a particular concern when the outsourcing is to foreign countries in which manufacturers may be subject to less strict safety standards than in the U.S. or in those countries to which products are intended to be ultimately distributed. The same applies where substantial portions of intermediate products, parts, or basic commodities are purchased from third parties. Where material to

Volume 42, Number 2, April 2009.

the company, the board should be informed about the company's program and review it periodically as part of its risk oversight role.

Health and Safety

Companies may be subject to an array of laws and regulations designed to ensure the safety of their facilities, and a safety management system designed to comply with these requirements should be part of a company's risk management structure. Failure to do so can expose the company to legal liability, fines, and reputational damage. For example, BP recently settled more than 4,000 injury and property-damage claims generated by a major explosion at its Texas oil refinery. Following an investigation, the BP U.S. Refineries Independent Safety Review Panel, a panel constituted by the U.S. Chemical Safety and Hazard Investigation Board and led by former Secretary of State James Baker, concluded that BP's executive management and its refining line management had failed to ensure the implementation of an "integrated, comprehensive, and effective" process safety management system and that BP's board "had not ensured, as a best practice, that management did so." As part of risk management oversight, the board or relevant committee should review with management the programs in place to maintain the company's facilities in compliance with relevant legal standards and provide adequate safety training for employees.

Environmental

Environmental risk stems from compliance issues under the many environmental laws and regulations that may apply to the company and liability exposure from private lawsuits claiming damages in connection with polluting activity. Environmental compliance has also received increasing scrutiny in the political arena from governmental and nongovernmental organizations and in the public media. Environmental laws and regulations may also impose strict liability on companies, under which a company may be responsible for remediation of environmental problems relating to property it owns, even if the pollution was caused by prior owners. In addition to the monetary or remedial liabilities that may be imposed for non-compliance with environmental requirements or polluting activities, a company can experience severe reputational damage, as in the case of the Exxon Valdez oil spill. Environmental risk, of course, will be more material to some companies than others, but understanding exposure to this risk should be part of the company's risk assessment process and overall risk management system.

Insurance

Insurance, both commercial insurance and self-insurance, covering operational risks is part of a company's risk management structure. In overseeing risk management, the company's board or relevant committee should be briefed on the company's insurance programs, the type and level of insurance coverage, and any material gaps in insurance. The review of the insurance program should also include a general understanding of the cost of insurance coverage, the creditworthiness of insurers, alternative risk transfer solutions, and how the company's insurance program compares to others in the industry, if known.

The board should also ensure that the company has up-to-date indemnification arrangements in place for board members and has purchased adequate director and officer (D&O) liability insurance. These arrangements should be reviewed periodically to give the board comfort as to the adequacy of the company's coverage. Retentions and exclusions in the D&O coverage should be explained to the board so that the directors understand where they have protection and where they do not.

Information Technology

Information technology (IT) risks may arise in the context of securing the reliability and functionality of the IT systems necessary to the company's business operations and with respect to ensuring the security and protection of customer and other data stored and processed by those systems. Failures of IT systems can cause major business disruption, including significant revenue and business losses, while breaches of IT system security can have legal consequences such as private lawsuits and regulatory restrictions caused by compliance issues with applicable data security regulations. Either can also cause significant reputational damage. In the context of data security and privacy regulation, it is also important to keep in mind foreign laws and regulations, such as consumer privacy laws in Europe that are significantly stricter than those in the U.S. Given the importance of information technology

to most companies today, information technology risk management will almost always be an important part of the company's overall risk management program.

Intellectual Property

Safeguarding the integrity of a company's intellectual property (IP) – including patents, trademarks and copyrights, trade secrets, know-how and not-yet-protected intellectual property – and preventing the misappropriation of another party's intellectual property are both important parts of overall risk management for many companies. Intellectual property can represent a significant portion of a company's value, particularly in R&D intensive industries or industries that rely on branded products or services. At the same time, IP rights face risks of appropriation and exploitation in today's environment, as they often are relatively easily accessible for other parties through the use of sophisticated technical means, such as spyware, or by partners in business relationships with whom the company works globally, such as in joint development or distribution cooperation, and who have access to intellectual property in the course of such cooperation.

For companies in which IP rights are a material part of the business, the risks to those rights and the programs to protect against such risks should be part of the company's risk management review. Management should review with the board or the relevant committee the company's organizational structures and procedures for IP protection, including: (1) proper recognition of inventions by employees, suppliers, joint ventures, and other parties; (2) transformation of inventions into protected intellectual property rights of the company; (3) adequate protection of trade secrets against misappropriation or loss of knowledge by or to employees, consultants, partners, suppliers, vendors, or other third parties; (4) appropriate processes to register and defend patent and other IP rights; and (5) sufficient diligence processes to avoid the infringement of other parties' protected IP rights.

Antitrust Compliance

Charges of price-fixing, the abuse of a dominant position and other anticompetitive practices that violate U.S. and other antitrust laws can carry with them the prospect of lengthy government investigations, heavy fines, reputational damage, and exposure to private lawsuits. For companies with material international operations, this is also true with respect to foreign antitrust laws and regulations. For example, Microsoft was fined approximately €497 million by the EU for alleged abuse of its dominant position in the EU market, and the European Commission recently imposed its highest-ever cartel penalty of more than €1.3 billion on a group of companies delivering automotive glass in Europe. Thus, antitrust compliance policies and procedures should be part of the company's overall risk management structure, and an overview of these compliance programs should be part of the review of risk management with the board or relevant committee.

Employment Practices

Employment-related claims are most commonly based on alleged discrimination, sexual and workplace harassment, wrongful termination, emotional distress, misrepresentation, written or oral defamation, and retaliation against whistle-blowers. Such claims can carry exposure to monetary damages and risk reputational damage. To protect against these risks, companies should have clear policies and procedures for hiring, promotion, and compensation and robust programs for educating supervising employees about their legal obligations. The policies should be regularly reviewed and updated to reflect the most recent legal developments and should be clearly documented in employee handbooks and other sources of employee information. In addition to compliance with employment laws and regulations, attention should also be given, as noted above, to the incentives that a company's compensation structure may create with respect to risk-taking and risk-avoidance behavior.

Social Responsibility and Human Rights

A company's alleged complicity in human rights violations in foreign countries where the company does business can expose the company both to legal liability and to reputational damage. The suit filed by the Presbyterian Church of Sudan against Talisman Energy in 2001 for its alleged complicity in atrocities committed by the Sudanese government is an example. Although Talisman's motion for summary judgment was granted in 2006, the allegations were covered extensively in the press and mired Talisman in legal proceedings for several

Volume 42, Number 2, April 2009.

years. Social responsibility is also increasingly a subject for shareholder activism, with the attendant publicity that this can entail. There are also indications that companies may come under increasing political pressure to focus attention on social responsibility and human rights in the operation of their business in the future. For example, in June 2008 a report presented to the United Nations Human Rights Council proposed that companies bear the "responsibility to respect human rights," that the state has a "duty to protect" against human rights abuses by companies, and that both the state and businesses must provide more effective access to remedies for human rights violations. Under the proposal, in order to discharge their responsibility to respect human rights, companies would be required to conduct a broad due diligence process "to become aware of, prevent and address adverse human rights impacts" in the same way that companies must "assess and manage financial and related risks."

IV. 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 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 committee.

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

Dedicated Committee or Subcommittee or Dedicated Meeting Times

Currently, 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. In many companies, however, the scope and complexity of risk management may make it desirable to consider creating a dedicated risk management committee or subcommittee in order to permit greater focus at the board level on risk management and oversight. The NYSE rule permits boards to delegate the primary risk oversight function to a separate board committee, subject to limited continuing audit committee oversight. Currently, it appears that less than five of the one hundred largest U.S. companies by market capitalization maintain a board committee dedicated to risk management; however, in light of the intense focus on risk in the current environment, this number will likely increase in the future.

Depending on the company, the audit committee may not always be best suited to take the lead in overseeing risk management at the board level. Given the myriad obligations specifically mandated or delegated to it by law and regulations, the audit committee typically has an already crowded agenda and may not have sufficient time to devote to optimal risk oversight. Moreover, the audit committee's focus on compliance with auditing and accounting standards is not necessarily the right focus for identifying and assessing the broad array of risks that the company may face. Indeed, it is quite possible for strict compliance with accounting rules to mask risk, as occurred with the creation of structured investment vehicles and other off-balance sheet entities.

If the company keeps the 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 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.

Risk Oversight Role of the Full Board and Other Committees

While the primary board-level risk oversight role is typically allocated to a committee – whether

a dedicated committee or subcommittee or the audit committee – the full board should also receive information about the company's risk management system and the most significant risks that the company faces. This can be accomplished through reports from the committee charged with risk management oversight and/or abbreviated versions of the briefings provided by management and advisors to the committee.

In addition, 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, as noted above, the company's compensation structure should be reviewed and, if necessary, revised 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.

Board Training

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 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 on the number of outside boards they serve on. One result of these trends, however, is that companies often have a number of directors who come to board service without any detailed knowledge of the industry in which the company operates and/or without direct experience in private sector management. This makes director training, as discussed above, all the more important. But 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 the committee charged with risk management oversight.

In addition, 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. 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 committee, actual membership on the board may be an effective means of obtaining regular, consistent and ongoing input from such executives at the board level.

Lines of Communication

The ability of the board or relevant 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 management executives 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 need to be proactive in asking for more.

The committee charged with risk oversight should have sessions in which they meet directly with the 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 be comfortable in informing the board or relevant committee of extraordinary risk issues and developments that need the immediate attention of the board outside of the regular reporting procedures. As discussed above, the committee charged with risk oversight should also report on its discussions and findings to the full board on a periodic basis.

Legal Compliance Programs and Corporate Culture

Senior management should provide the board or relevant committee with an appropriate review of the company's legal compliance programs and how they are designed to address the company's risk profile. 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.

In addition to the formal compliance program, the board or relevant committee should also encourage management to promote a corporate culture that understands risk management and incorporates it into its overall corporate strategy and its day-to-day business operations. Risk management should not be viewed as an impediment to corporate progress, or isolated as a specialized corporate function, but instead 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.

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. Anticipating future risks is obviously a key element of avoiding or mitigating those risks before they become crises. In reviewing risk management, the board or relevant committee 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.

