February 14, 2017

Risk Management and the Board of Directors (Revised February 2017)

I. INTRODUCTION

Overview

The year 2017 begins amid significant shifts in the world's geopolitical order. Recent events such as the U.S. Presidential election and the United Kingdom's historic vote to leave the European Union have brought with them a great deal of both political and economic uncertainty. At the same time, the ever-increasing dependence on technological advances characterizing all aspects of business and modern life has been accompanied by a rapidly growing threat of cyberattack and cyberterrorism, including to the world's most critical commercial infrastructure. As political and commercial leaders grapple with these new realities, corporate risk taking and the monitoring of corporate risk continue to take prominence in the minds of boards of directors, investors, legislators and the media. Major institutional shareholders and proxy advisory firms now evaluate risk oversight matters when considering withhold votes in uncontested director elections and routinely engage companies on risk-related topics. This focus on risk management has also led to increased scrutiny of the relationship between compensation arrangements throughout the organization and excessive risk taking. Risk management is no longer simply a business and operational responsibility of management. It has also become a governance issue that is squarely within the purview of the board. Accordingly, oversight of risk should be an area of regular board assessment. This overview highlights a number of issues that have remained critical over the years and provides an update to reflect emerging and recent developments.

Both the law and practicality continue to support the proposition that the board cannot and should not be involved in actual day-to-day risk *management*. Directors should instead, through their risk *oversight* role, satisfy themselves that the risk management policies and procedures designed and implemented by the company's senior executives and risk managers are consistent with the company's strategy and risk appetite; that these policies and procedures are functioning as directed; and that necessary steps are taken to foster an enterprise-wide culture that supports appropriate risk awareness, behaviors and judgments about risk and recognizes and appropriately escalates and addresses risk-taking beyond the company's determined risk appetite. The board should be aware of the type and magnitude of the company's principal risks and should require that the CEO and the senior executives are fully engaged in risk management. Through its oversight role, the board can send a message to management and employees that

comprehensive risk management is not an impediment to the conduct of business nor a mere supplement to a firm's overall compliance program. Instead, it is an integral component of strategy, culture and business operations. In addition, the roles and responsibilities of different board committees in overseeing specific categories of risk should be reviewed to ensure that, taken as a whole, the board's oversight function is coordinated and comprehensive. In that regard, a recent PricewaterhouseCoopers' survey of directors reported that 83% of directors believe there is a clear allocation of risk oversight responsibilities among the board and its committees, but nearly 20% of the directors surveyed suggested the clarity of the allocation of these responsibilities could still be improved.

Cybersecurity's Increasing Importance

Cybersecurity has been producing more and more headlines in recent years, and 2016 continued this trend. According to a study performed by Symantec, the identities of over 429 million people were wrongfully exposed through cyberattacks last year. As recent examples (*e.g.,* the hacking of computer networks belonging to the Democratic National Committee) have highlighted, online security breaches, theft of personal data, proprietary or commercially sensitive information and damage to IT infrastructure are omnipresent threats and can have a significant financial and reputational impact on companies and organizations. In today's highly technological world, virtually all company functions across all industries utilize some form of information technology. Industry-leading experts recommend that in order to be effective, companies must not only have an effective and well-vetted cybersecurity breach response plan, but such plans must also be periodically tested in simulated situations to ensure that key personnel understand their precise roles and the real-time decisions that must be made.

Lawmakers and regulators have recently focused their attention on cybersecurity risk. In October 2016, federal banking regulators sought comments (due in early 2017) on enhanced cyber risk-management standards for major financial institutions. In addition, the New York State Department of Financial Services (DFS) announced in 2016 detailed regulations requiring covered institutions—entities authorized under New York State banking, insurance or financial services laws—to meet strict minimum cybersecurity standards, and the Department of Treasury's Financial Crimes Enforcement Network (FinCEN) issued an advisory on the reporting of cyber events under the Bank Secrecy Act. On December 28, 2016, DFS released revised regulations (see our previous memorandum here), which, subject to notice and comment, are set to become effective on March 1, 2017. In May 2016, federal legislation regarding the

application of the Sarbanes-Oxley Act of 2002 (SOX) certifications and internal controls requirements to a company's information and technology systems and cybersecurity-related controls, and whether companies must publicly explain why they do not have at least one director with specific cybersecurity-related expertise, was referred to the House Committee of Financial Services. As of the date of this publication, such proposed legislation has not moved out of committee.

The SEC has recently voiced its support of the Framework for Improving Critical Infrastructure Cybersecurity released by the National Institute of Standards and Technology (NIST) and indicated that as part of fulfilling their risk oversight function, boards should at a minimum work with management to ensure that corporate policies are in-line with the Framework's guidelines. The Framework is divided into three central components: the Framework core (*i.e.,* a set of cybersecurity activities and informative references that are organized around particular outcomes designed to enable communication of cyber risk across an entire organization); the Framework profile (*i.e.,* the alignment of industry standards and best practices to the Framework core in particular implementation scenarios which supports prioritization and measurement in conjunction with factoring in relevant business needs); and the Framework implementation tiers (*i.e.,* a description of how cybersecurity risk is managed by an organization and the degree to which the risk management practices exhibit key characteristics). On January 10, 2017, NIST released, and is seeking public comment on, proposed updates to the Framework. In addition to the NIST Framework, the International Organization for Standardization (ISO), an independent, non-governmental international organization, published its own information security standard known as the ISO/IEC 27001, which provides a similar framework for cybersecurity implementation.

Strong Institutional Investor Focus

The focus on risk management is a top governance priority of institutional investors. A PricewaterhouseCoopers survey report issued in 2014 indicated that risk management was a top priority for investors, and a 2016-2017 National Association of Corporate Directors (NACD) survey revealed that one in ten boards that met with institutional investors specifically discussed risk oversight. In exceptional circumstances, this scrutiny can translate into shareholder campaigns and adverse voting recommendations from ISS. ISS will recommend voting "against" or "withhold" in director elections, even in uncontested elections, when the company has experienced certain extraordinary circumstances, including material failures of risk oversight. In 2012, ISS clarified that such failures of risk oversight will include bribery, large or serial fines or

sanctions from regulatory bodies and significant adverse legal judgments or settlements. Thus, in connection with the ongoing FCPA investigation at Wal-Mart, ISS recommended voting against the chairman, CEO and audit committee chair "due to the board's failure to adequately communicate material risk factors to shareholders, and to reassure shareholders that the board was exercising proper oversight and stewardship and would hold executives accountable if appropriate." ISS has made similar withhold recommendations at other companies, too, in connection with perceived risk oversight issues.

Tone at the Top and Corporate Culture

The board and relevant committees should work with management to promote and actively cultivate a corporate culture and environment that understands and implements enterprise-wide risk management. Comprehensive risk management should not be viewed as a specialized corporate function, but instead should be treated as an integral, enterprise-wide component that affects how the company measures and rewards its success.

The assessment of risk, the accurate evaluation of risk versus reward and the prudent mitigation of risk should be incorporated into all business decision-making. In setting the appropriate "tone at the top," transparency, consistency and communication are key: the board's vision for the corporation, including its commitment to risk oversight, ethics and intolerance of compliance failures, should be communicated effectively throughout the organization. As noted in a 2014 speech by former SEC Chair Mary Jo White, "[e]nsuring the right 'tone at the top' . . . is a critical responsibility for each director and the board collectively." Risk management policies and procedures and codes of conduct and ethics should be incorporated into the company's strategy and business operations, with appropriate supplementary training programs for employees and regular compliance assessments.

II. THE RISK OVERSIGHT FUNCTION OF THE BOARD OF DIRECTORS

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

Fiduciary Duties

The Delaware courts have taken the lead in formulating the national legal standards for directors' duties for risk management. The Delaware courts

have developed the basic rule under the *Caremark* line of cases that directors can only be liable for a failure of board oversight where there is "sustained or systemic failure of the board to exercise oversight—such as an utter failure to attempt to assure a reasonable information and reporting system exists," noting that this is a "demanding test." *In re Caremark International Inc. Derivative Litigation*, 698 A.2d 959, 971 (Del. Ch. 1996). Delaware Court of Chancery decisions since *Caremark* have expanded upon that holding, while reaffirming its fundamental standard. The plaintiffs in *In re Citigroup Inc. Shareholder Derivative Litigation*, decided in 2009, alleged that the defendant directors of Citigroup had breached their fiduciary duties by not properly monitoring and managing the business risks that Citigroup faced from subprime mortgage securities, and by ignoring alleged "red flags" that consisted primarily of press reports and events indicating worsening conditions in the subprime and credit markets. The court dismissed these claims, reaffirming the "extremely high burden" plaintiffs face in bringing a claim for personal director liability for a failure to monitor business risk and that a "sustained or systemic failure" to exercise oversight is needed to establish the lack of good faith that is a necessary condition to liability.

In *In re The Goldman Sachs Group, Inc. Shareholder Litigation*, decided in October 2011, the court dismissed claims against directors of Goldman Sachs based on allegations that they failed to properly oversee the company's alleged excessive risk taking in the subprime mortgage securities market and caused reputational damage to the company by hedging risks in a manner that conflicted with the interests of its clients. Chief among the plaintiffs' allegations was that Goldman Sachs' compensation structure, as overseen by the board of directors, incentivized management to take on ever riskier investments with benefits that inured to management but with the risks of those actions falling to the shareholders. In dismissing the plaintiffs' *Caremark* claims, the court reiterated that, in the absence of "red flags," the manner in which a company evaluates the risks involved with a given business decision is protected by the business judgment rule and will not be second-guessed by judges.

Overall, these cases reflect that it is difficult to show a breach of fiduciary duty for failure to exercise oversight and that the board is not required to undertake extraordinary efforts to uncover non-compliance within the company, provided a monitoring system is in place. Nonetheless, while it is true that the Delaware Supreme Court has not indicated a willingness, to date, to alter the strong protection afforded to directors under the business judgment rule which underpins *Caremark* and its progeny, boards should keep in mind that cases involving particularly egregious facts and circumstances and substantial shareholder losses

necessarily risk more unfavorable outcomes, particularly in cases brought outside of Delaware. Companies should adhere to reasonable and prudent practices and should not structure their risk management policies around the minimum requirements needed to satisfy the business judgment rule.

Federal Laws and Regulations

Dodd-Frank. The Dodd-Frank Act created new federally mandated risk management procedures principally for financial institutions. Dodd-Frank requires bank holding companies with total assets of $10 billion or more, and certain other non-bank financial companies as well, to have a separate risk committee which includes at least one risk management expert with experience managing risk of large companies.

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

The SEC proxy rules also require a company to discuss the extent to which risks arising from a company's compensation policies are reasonably likely to have a "material adverse effect" on the company. A company must further discuss how its compensation policies and practices, including those of its non-executive officers, relate to risk management and risk-taking incentives.

Industry-Specific Guidance and General Best Practices Manuals

Various industry-specific regulators and private organizations publish suggested best practices for board oversight of risk management. Examples include reports by the National Association of Corporate Directors (NACD)—Blue Ribbon Commission on Risk Governance, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and the Business Roundtable's 2016 Principles of Corporate Governance. The 2009 NACD report provides guidance on, and principles for, the board's risk oversight activities, the relationship between strategy and risk and the board's role in relation to particular categories of risk. These principles include understanding key drivers of success

and risks in the company's strategy, crafting the right relationship between the board and its standing committees as to risk oversight, establishing and providing appropriate resources to support risk management systems, monitoring potential risks in the company's culture and incentive systems and developing an effective risk dialogue with management.

In June 2016, COSO sought public comment on a draft of an updated version of its internationally recognized enterprise risk management framework, which it originally released in 2004. The comment period concluded in October 2016. As proposed to be revised, the COSO approach presents five interrelated components of risk management: risk governance and culture (the tone of the organization); setting objectives; execution risk (the assessment of risks that may impact achievement of strategy and business objectives); risk information, communication and reporting; and monitoring enterprise risk management performance. Additional changes proposed to be adopted in the revised framework are a simplified definition of enterprise risk management designed to be accessible to personnel not directly involved in risk management roles; a clear examination of the role of culture; an elevated discussion of strategy; a renewed emphasis between risk and value; an enhanced alignment between performance and enterprise risk management; a more explicit linking of enterprise risk management to decision-making; an enhanced focus on the integration of enterprise risk management; a refined explanation of the concept of risk appetite and acceptable variation in performance (*i.e.,* risk tolerance); and a clear delineation between enterprise risk management and internal controls. A COSO 2009 enterprise risk management release recommends concrete steps for boards, such as understanding a company's risk philosophy and concurring with its risk appetite, reviewing a company's risk portfolio against that appetite and knowing the extent to which management has established effective enterprise risk management and is appropriately responding in the face of risk. In its 2010 progress report, COSO recommends that the board focus, at least annually, on whether developments in a company's business or the overall business environment have "resulted in changes in the critical assumptions and inherent risks underlying the organization's strategy." By understanding and emphasizing the relationship between critical assumptions underlying business strategy and risk management, the board can strengthen its risk oversight role.

In June 2015, The Conference Board Governance Center published a report, The Next Frontier for Boards: Oversight of Risk Culture, that contains useful recommendations for board-driven risk governance. Among other useful suggestions, the report suggests that boards receive periodic briefings (whether

from chief internal auditors, outside subject matter experts or consulting firms) on board oversight of risk culture expectations.

The Business Roundtable's 2016 Principles of Corporate Governance includes a set of seven "Guiding Principles of Corporate Governance," one of which is that the board approve corporate strategies that are intended to build long-term value and growth. As part of that function, the board should allocate capital for assessing and managing risks and set a "tone at the top" for ethical conduct. In describing the board's key responsibilities, the report also suggests that boards should understand the inherent risks in the company's strategic plan and how risks are being managed and, consistent with the COSO release, suggests that the board work with senior management to agree on the company's risk appetite and satisfy itself that the company's strategy is consistent with it.

III. RECOMMENDATIONS FOR IMPROVING RISK OVERSIGHT

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

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

- review with management the company's risk appetite and risk tolerance, the ways in which risk is measured on an aggregate, company-wide basis, the setting of aggregate and individual risk limits (quantitative and qualitative, as appropriate), the policies and procedures in place to hedge against or mitigate risks and the actions to be taken if risk limits are exceeded;

- establish a clear framework for holding the CEO accountable for building and maintaining an effective risk appetite framework and providing the board with regular, periodic reports on the company's residual risk status;

- 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, mitigating measures and action plans to be employed if a given risk materializes;

- review with management the assumptions and analysis underpinning the determination of the company's principal risks and whether adequate procedures are in place to ensure that new or materially changed risks are properly and promptly identified, understood and accounted for in the actions of the company;

- 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 company's executive compensation structure to ensure it is appropriate in light of the company's articulated risk appetite and risk culture and to ensure it is creating proper incentives in light of the risks the company faces;

- review the risk policies and procedures adopted by management, including procedures for reporting matters to the board and appropriate committees and providing updates, in order to assess whether they are appropriate and comprehensive;

- review management's implementation of its risk policies and procedures, to assess whether they are being followed and are effective;

- review with management the quality, type and format of risk-related information provided to directors;

- review the steps taken by management to ensure adequate independence of the risk management function and the processes for resolution and escalation of differences that might arise between risk management and business functions;

- review with management the design of the company's risk management functions, as well as the qualifications and backgrounds

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 primary elements comprising the company's risk culture, including establishing "a tone from the top" that reflects the company's core values and the expectation that employees act with integrity and promptly escalate non-compliance in and outside of the organization; accountability mechanisms designed to ensure that employees at all levels understand the company's approach to risk as well as its risk-related goals; an environment that fosters open communication and that encourages a critical attitude towards decision-making; and an incentive system that encourages, rewards and reinforces the company's desired risk management behavior;

- 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 senior management (and to the board or board committees as appropriate); and

- review reports from management, independent auditors, internal auditors, legal counsel, regulators, stock analysts and outside experts as considered appropriate regarding risks the company faces and the company's risk management function, and consider whether, based on individual director's experience, knowledge and expertise, the board or committee primarily tasked with carrying out the board's risk oversight function is sufficiently equipped to oversee all facets of the company's risk profile—including specialized areas such as cybersecurity—and determine whether subject-specific risk education is advisable for such directors.

In addition to considering the foregoing measures, the board may also want to focus on identifying external pressures that can push a company to take excessive risks and consider how best to address those pressures. In particular,

companies have come under increasing pressure in recent years from hedge funds and activist shareholders to produce short-term results, often at the expense of longer-term goals. These demands may include steps that would increase the company's risk profile, for example, through increased leverage to repurchase shares or pay out special dividends, or spinoffs that leave the resulting companies with smaller capitalizations. While such actions may make sense for a specific company under a specific set of circumstances, the board should focus on the risk impact and be ready to resist pressures to take steps that the board determines are not in the company's or shareholders' best interest.

Special Considerations Regarding Cybersecurity Risk

As cybersecurity risk continues to rise in prominence, so too has the number of organizations that have begun to specifically situate cybersecurity and cyber risk within their internal audit function. A 2016 Internal Audit Capabilities and Needs Survey, conducted by Protiviti, found that 73% of the organizations surveyed now include cybersecurity risk as part of their internal audit function, a 20% increase from 2015. Directors should assure themselves that their organization's internal audit function is performed by individuals who have appropriate technical expertise and sufficient time and other resources to devote to cybersecurity risk. Further, these individuals should understand and periodically test the organization's risk mitigation strategy, and provide timely reports on cybersecurity risk to the audit committee of the board. In addition to the considerations discussed above, boards should, in satisfying their risk oversight function with respect to cybersecurity, evaluate their company's preparedness for a possible cybersecurity breach, as well as the company's action plan in the event that a cybersecurity breach occurs. With respect to preparation, boards should consider the following actions, several of which are also addressed in The Conference Board's "A Strategic Cyber-Roadmap for the Board" released in November 2016:

- identify the company's "Crown Jewels"—*i.e.,* the company's mission-critical data and systems—and work with management to apply appropriate measures outlined in the NIST Framework;

- ensure that an actionable cyber incident response plan is in place that, among other things, identifies critical personnel and designates responsibilities; includes procedures for containment, mitigation and continuity of operations; and identifies necessary notifications to be issued as part of a preexisting notification plan;

- ensure that the company has developed effective response technology and services (*e.g.*, off-site data back-up mechanisms, intrusion detection technology and data loss prevention technology);

- ensure that prior authorizations are in place to permit network monitoring;

- ensure that the company's legal counsel is conversant with technology systems and cyber incident management to reduce response time; and

- establish relationships with cyber information sharing organizations and engage with law enforcement before a cybersecurity incident occurs.

Situating the Risk Oversight Function

Most boards delegate oversight of risk management to the audit committee, which is consistent with the NYSE rule that requires the audit committee to discuss policies with respect to risk assessment and risk management. In practice, this delegation to the audit committee may become more of a coordination role, at least insofar as certain kinds of risks will naturally be addressed across other committees as well (*e.g.,* risks arising from compensation structures are frequently considered in the first instance by the compensation committee). Financial companies covered by Dodd-Frank must have dedicated risk management committees. The appropriateness of a dedicated risk committee at other companies will depend on the industry and specific circumstances of the company. Boards should also bear in mind that different kinds of risks may be best suited to the expertise of different committees—an advantage that may outweigh any benefit from having a single committee specialize in risk management, so long as overall risk oversight efforts are properly coordinated and communicated. In recent years, the number of boards that have created a separate risk committee has grown. According to a 2016 Ernst & Young survey of S&P 500 companies, more than 75% of boards have at least one committee in addition to the mandatory committees, up from 61% in 2013, and of such boards, 11% have a separate risk committee. To date, however, separate risk committees remain uncommon outside the financial industry (according to the same Ernst & Young survey, of companies that have a separate risk committee, 73% are in the financial industry followed by 6% for industrials). Regardless of the delegation of risk oversight to committees, 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.

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.

Risk management issues may arise in the context of the work of other committees, and the decision-making in those committees should take into account the company's overall risk management system. Specialized committees may be tasked with specific areas of risk exposure. Banks, for instance, often maintain credit or finance committees, while energy companies may have public policy committees largely devoted to environmental and safety issues. Fundamental risks to the company's business strategy and risks facing the industries in which the company operates are often discussed at the full board level. Where different board committees are responsible for overseeing specific risks, the work of these committees should be coordinated in a coherent manner both horizontally and vertically so that the entire board can be satisfied as to the adequacy of the risk oversight function and the company's overall risk exposures are understood, including with respect to risk interrelationships. It may also be appropriate for the committee charged with risk oversight to meet in executive session both alone and together with other independent directors to discuss the company's risk culture, the board's risk oversight function and key risks faced by the company.

The board should formally undertake an annual review of the company's risk management system, including a review of board- and committee-level risk oversight policies and procedures, a presentation of "best practices" to the extent relevant, tailored to focus on the industry or regulatory arena in which the company operates, and a review of other relevant issues such as those listed above. To this end, it may be appropriate for boards and committees to engage outside consultants to assist them in both the review of the company's risk management systems and also assist them in understanding and analyzing business-specific risks. But because risk, by its very nature, is subject to constant and unexpected change, boards should keep in mind that annual reviews do not replace the need to regularly assess and reassess their own operations and processes, learn from past mistakes and seek to ensure that current practices enable the board to address specific major issues whenever they may arise. Where a

major or new risk comes to fruition, management should thoroughly investigate and report back to the full board or the relevant committees as appropriate.

Lines of Communication and Information Flow

The ability of the board or a committee to perform its oversight role is, to a large extent, dependent upon the relationship and the flow of information between the directors, senior management and the risk managers in the company. If directors do not believe they are receiving sufficient information—including information regarding the external and internal risk environment, the specific material risk exposures affecting the company, how these risks are assessed and prioritized, risk response strategies, implementation of risk management procedures and infrastructure and the strengths 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 type, format and frequency of risk information required by the board. High-quality, timely and credible information provides the foundation for effective responses and decision-making by the board.

Any committee charged with risk oversight should hold sessions in which it meets directly with key executives primarily responsible for risk management, just as an audit committee meets regularly with the company's internal auditors and liaises with senior management in connection with CEO and CFO certifications for each Form 10-Q and Form 10-K. In addition, senior risk managers and senior executives should understand they are empowered to inform the board or committee of extraordinary risk issues and developments that need the immediate attention of the board outside of the regular reporting procedures. In light of the *Caremark* standards discussed above, the board should feel comfortable that "red flags" or "yellow flags" are being reported to it so that they may be investigated if appropriate.

Legal Compliance Programs

Senior management should provide the board or committee with an appropriate review of the company's legal compliance programs and how they are designed to address the company's risk profile and detect and prevent wrongdoing. While compliance programs will need to be tailored to the specific company's needs, there are a number of principles to consider in reviewing a program. As noted earlier, there should be a strong "tone at the top" from the board and senior management emphasizing that non-compliance will not be tolerated. This cultural element is taking on increasing importance and receiving heightened attention from regulators as well. A well-tailored compliance program and a culture that

values ethical conduct continue to be critical factors that the Department of Justice will assess under the Federal Sentencing Guidelines in the event that corporate personnel engage in misconduct. In addition, the DOJ's heightened focus on individual accountability for wrongdoing deriving from the 2015 "Yates memo" is likely to remain a feature of the enforcement landscape, thus magnifying the importance of responding in an appropriate manner to indications of possible misconduct.

A compliance program should be designed by persons with relevant expertise and will typically include interactive training as well as written materials. Compliance policies should be reviewed periodically in order to assess their effectiveness and to make any necessary changes. There should be consistency in enforcing stated policies through appropriate disciplinary measures. Finally, there should be clear reporting systems in place both at the employee level and at the management level so that employees understand when and to whom they should report suspected violations and so that management understands the board's or committee's informational needs for its oversight purposes. A company may choose to appoint a chief compliance officer and/or constitute a compliance committee to administer the compliance program, including facilitating employee education and issuing periodic reminders. If there is a specific area of compliance that is critical to the company's business, the company may consider developing a separate compliance apparatus devoted to that area.

Anticipating Future Risks

The company's risk management structure should include an ongoing effort to assess and analyze the most likely areas of future risk for the company, including how the contours and interrelationships of existing risks may change and how the company's processes for anticipating future risks are developed. Anticipating future risks is a key element of avoiding or mitigating those risks before they escalate into crises. In reviewing risk management, the board or relevant committees should ask the company's executives to discuss the most likely sources of material future risks and how the company is addressing any significant potential vulnerability.

Martin Lipton
Daniel A. Neff
Andrew R. Brownstein
Steven A. Rosenblum
Adam O. Emmerich
Wayne M. Carlin
Sabastian V. Niles
Marshall L. Miller
Sebastian L. Fain
David J. Cohen