August 31, 2018

Risk Management and the Board of Directors (Updated August 2018)

I. INTRODUCTION

Overview

Political, legal and economic arenas in the U.S. and around the world have continued to evolve in response to rapidly advancing technologies. Innovation, new business models and dealmaking are transforming competitive and industry landscapes and impacting companies' strategic plans and prospects for sustainable, long-term value creation. Tax reform has created new opportunities and challenges for companies as well. Meanwhile, the severe consequences that can flow from misconduct within an organization continue to serve as a reminder that corporate operations are fraught with risk. Social and environmental issues, including the focus on income inequality and economic disparities, scrutiny of sexual misconduct issues and evolving views on climate change and natural disasters, have become increasingly salient in the public sphere, requiring companies to exercise utmost care to address legitimate issues and avoid public relations crises and liability.

Corporate risk taking and the monitoring of corporate risk remain prominently top of mind for boards of directors, investors, legislators and the media. Major institutional shareholders and proxy advisory firms increasingly 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 compensation arrangements throughout the organization that have the potential for incentivizing 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 oversight responsibility of the board. This memorandum highlights a number of issues that have remained critical over the years and provides an update to reflect emerging and recent developments. Key topics addressed in this memorandum include:

- the distinction between risk oversight and risk management;
- a lesson from Wells Fargo on risk oversight;
- the strong institutional investor focus on risk matters;

- tone at the top and corporate culture;
- fiduciary duties, legal and regulatory frameworks and third-party guidance on best practices;
- specific recommendations for improving risk oversight;
- legal compliance programs;
- special considerations regarding cybersecurity matters;
- special considerations pertaining to environmental, social and governance (ESG) risks; and
- anticipating future risks.

Risk Oversight by the Board – Not Risk Management

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. A Deloitte January 2018 survey of board members confirmed that a wide range of risk topics regularly fill boardroom agendas, and a 2017 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 clarity about the allocation of these responsibilities could still be improved.

A Lesson from Wells Fargo on Risk Oversight

On February 2, 2018, the Federal Reserve issued an enforcement action against Wells Fargo, which, among other things, contained several statements regarding the Federal Reserve's view on the responsibility that boards of directors have with respect to risk management. The Federal Reserve:

- characterized compliance breakdowns as failures of governance and board oversight;
- noted replacement of board members;
- censured directors with publicly released letters of reprimand even after they had left the board for "lack of inquiry and lack of demand for additional information";
- expressed the view that a board's composition, governance structure and practices should support the company's business strategy and be aligned with risk tolerances;
- expressed the view that business growth strategies be supported by a system for managing all key risks, including those arising from performance pressure and compensation incentive systems and the potential that business goals could motivate compliance violations and improper practices;
- expressed the view that "management assurances" of enhanced monitoring and handling of known misconduct be backed up by "detailed and concrete plans" reported to the board; and
- referred to the company's published corporate governance guidelines as containing duties and responsibilities that were not fulfilled.

While the Federal Reserve's regulatory authority over banks enables it to impose greater responsibility for risk management on bank directors than is imposed by state corporation law on directors of non-bank corporations, it is important to note the Federal Reserve's views in the Wells Fargo matter as they will undoubtedly be cited and argued in future non-bank cases. Companies should reflect on the expectations on the board with respect to assuring that appropriate

risk management systems are in place. This includes setting high expectations for General Counsels and compliance departments, as well as following up with robust and prompt inquiry when evidence emerges of material compliance breakdowns.

Strong Institutional Investor Focus

The focus on risk management is a top governance priority of institutional investors. In recent years, investors have pushed for more meaningful and transparent disclosures on boards' activities and performance with respect to risk oversight, and a recent National Association of Corporate Directors (NACD) survey revealed that more than one in ten boards whose directors met with institutional investors specifically discussed risk oversight with these investors.

Vanguard has become particularly active in engaging with boards on the topic of risk oversight. In August 2017, Vanguard published several letters and reports that outlined four pillars underlying its evaluation of corporate governance practices, with the fourth pillar explicitly being risk oversight, on the theory that "directors are shareholders' eyes and ears on risk" and "shareholders rely on a strong board to oversee the strategy for realizing opportunities and mitigating risks." Vanguard reiterated this sentiment in its recently published 2018 Investment Stewardship Annual Report and stated that in 2018 alone, the number of conversations Vanguard had with boards on risk oversight nearly doubled. In the report, Vanguard remarked that while corporate governance has improved on many fronts, 2018 also featured some "large-scale failures of governance," with many companies "engulfed in controversy—from cybersecurity breaches to systemic business practices that treated customers unfairly to sexual harassment and other forms of gender discrimination." In the wake of these recent corporate governance controversies, Vanguard indicated that in its engagement with companies, the indexing giant wants to know what reasonable steps a board has taken to review and improve its risk oversight practices, and that boards should expect that Vanguard will ask questions such as:

- How do management and the board oversee risk? How frequently do risk conversations take place, and who participates?
- What type of risk reporting does the board receive? How often?
- How does the board ensure it is hearing independent external perspectives, especially ones that may differ from the views of management?

- How does the board identify "red flags" that alert it to potential areas of concern? How does the board ensure that these matters are elevated to the board just as swiftly as positive news?

- Given that a board meets only periodically through the year, and often only with management, what specific steps does the board take to understand the company's business culture and ensure that it reflects the company's espoused values?

In exceptional circumstances, this scrutiny from institutional investors can translate into shareholder campaigns and adverse voting recommendations from proxy advisory firms such as Institutional Shareholder Services (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. ISS has noted that failures of risk oversight include, but are not limited to, bribery, large or serial fines or sanctions from regulatory bodies, significant adverse legal judgments or settlements and hedging of company stock. For example, ISS recommended in the 2017 proxy season that shareholders vote against 12 out of 15 Wells Fargo directors, including the company's independent chairman, on the theory that the board committees "tasked with risk oversight failed over a number of years to provide a timely and sufficient risk oversight process that should have mitigated the harmful impact of the unsound retail banking sales practices that occurred" during that time period. ISS has made negative director 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 2017 NACD Blue Ribbon Commission report, "[o]versight of corporate cultures should be among the top governance imperatives for every board, regardless of its size or sector." Risk management policies and procedures and codes of conduct and ethics should be incorporated into the company's strategy and business operations, including promotion and compensation procedures, with appropriate supplementary training programs for employees and regular compliance assessments.

Indeed, recent developments in response to reports of sexual misconduct in the workplace make clear that setting the appropriate "tone at the top" is perhaps more important than ever before. Sexual harassment can have a devastating impact, first and foremost, on the employees targeted by such predatory behavior. It can also have a significant impact on corporate culture, employee morale and retention, consumer preferences and public perception. In light of heightened media and public scrutiny, delayed or indecisive responses to sexual misconduct can often be as damaging to a company as the misconduct itself. Despite the serious risks associated with sexual harassment, many boards are still not adequately addressing whether they have the right policies and procedures in place to prevent sexually inappropriate behavior and/or sexism in the workplace. As revealed in a 2017 survey of 400 private and public company directors by Boardlist and Qualtrics, 88% of boards "had not implemented a plan of action as a result of recent revelations in the media," and 83% had not "re-evaluated the company's risks regarding sexual harassment or sexist behavior at the workplace."

It is important that the board consider its oversight role with respect to sexual harassment claims and be briefed on the factors used by management in determining which claims are reported to the board. The board should review the company's policies and procedures regarding sexual harassment or assault allegations, and may want to be briefed on the company's employee training program and protocols for addressing sexual misconduct. The board should also work with management to consider developing a crisis response plan that includes the participation of human resources, public relations and legal counsel.

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. Under the *Caremark* line of cases, these courts have held that directors can be liable for a failure of board oversight only 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.

In a 2017 decision dismissing *Caremark* claims, *Oklahoma Firefighters Pension & Retirement System* v. *Corbat*, the court emphasized that directors can only be held liable for a failure to act in the face of "red flags" where the inaction suggests "not merely inattention, but actual scienter. In other words, the conduct must imply that the directors are knowingly acting for reasons other

than the best interest of the corporation." The Delaware Supreme Court reaffirmed this standard and reached the same result in its 2017 majority decision in *City of Birmingham Retirement and Relief System* v. *Good*, which grew out of major environmental damage resulting from the collapse of a Duke Energy storm water pipe that caused extensive contamination of the Dan River and resulted in sanctions against the company. As the Court aptly put it: "[T]he question before us is not whether Duke Energy should be punished for its actions. That has already happened. What is before us is whether a majority of Duke Energy directors face a substantial likelihood that they will be found personally liable for intentionally causing Duke Energy to violate the law or consciously disregarding the law. We find, as the Court of Chancery did, that the plaintiffs failed to meet this pleading requirement." Nonetheless, a word of caution is warranted, as Chief Justice Strine in dissent would have reversed, concluding that at the pleading stage, the plaintiff had pleaded "facts supporting an inference that Duke consciously was violating the law, taking steps that it knew were not sufficient to come into good faith compliance, but which it believed would be given a blessing by a regulatory agency whose fidelity to the law, the environment, and public health, seemed to be outweighed by its desire to be seen as protecting Duke and the jobs it creates."

Another situation that tested the limits of the *Caremark* doctrine presented itself in *In re Wells Fargo & Company Shareholder Derivative Litigation*, also decided in 2017. There, a California court applying Delaware law, denied the defendants' motion to dismiss because the plaintiffs pointed to numerous "red flags" of which the company's directors allegedly were or should have been aware and took no substantial remedial steps. The plaintiffs asserted that Wells Fargo's directors knew or consciously disregarded that Wells Fargo employees were creating millions of deposit and credit card accounts for customers without the customers' knowledge or consent. The court rejected defense efforts to explain away the alleged "red flags" as "insignificant when viewed in their larger context." Rather than look at the "red flags" in isolation, as the defendants urged, the court viewed them collectively, finding that "Defendants ignore the bigger picture by addressing each of these "red flags" in piecemeal fashion." The court concluded that while the "red flags" might "appear relatively insignificant to a large company like Wells Fargo when viewed in isolation, when viewed collectively they support an inference that a majority of the Director Defendants consciously disregarded their fiduciary duties despite knowledge regarding widespread illegal account-creation activities, and . . . that there is a substantial likelihood of directors oversight liability."

Thus, while it is true that the Delaware Supreme Court has not indicated a willingness to alter the strong protection afforded to directors under the business judgment rule that underpins *Caremark* and its progeny, cases such as *In re Wells Fargo* and Chief Justice Strine's dissent in *Good* should serve as reminders that board processes and decision-making may still be questioned where there are specific allegations that directors ignored "red flags," particularly when the "red flags" pointed to issues that, often with the benefit of hindsight, could be viewed as reflecting significant problems. Companies should adhere to reasonable and prudent practices and should not structure their risk management policies around only the minimum requirements needed to satisfy the business judgment rule.

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. The SEC requires companies to disclose in their annual reports "factors that make an investment in a registrant's securities speculative or risky." While the SEC has emphasized that risk factor disclosures should be concise, there is a growing concern that the SEC's increasing disclosure requirements have made companies feel compelled to overdisclose and to provide "boilerplate" risk factors that have limited the utility of the disclosures. On April 3, 2016, the SEC began seeking public comment on a concept release to modernize and simplify business and financial disclosure requirements in Regulation S-K. In this regard, the SEC has proposed eliminating the risk factor examples provided in Item 503(c) of Regulation S-K, because "the inclusion of these examples could suggest that a registrant must address each one of its risk factor disclosures, regardless of the significance to its business." According to the SEC, eliminating such examples will encourage companies to provide less boilerplate risk factor disclosure.

The SEC also requires companies to disclose the board's role in risk oversight, the relevance of the board's leadership structure to such matters and 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.

Foreign Corrupt Practices Act. In November 2017, the Department of Justice announced a new FCPA enforcement policy that codified and enhanced a pilot program launched in April 2016. Under the pilot program, companies were eligible for a range of mitigation credit if they voluntarily self-reported FCPA misconduct; fully cooperated with the DOJ's investigation, including disclosing all relevant facts and identifying culpable individuals; and implemented timely and appropriate remedial measures. The pilot program, as intended, appears to have sparked an increase in the number of companies voluntarily disclosing FCPA-related misconduct to the DOJ, with seven companies receiving DOJ decisions not to prosecute due to their participation in the pilot program.

As a result of the pilot program's success, the DOJ formally adopted an enhanced version of the program to further encourage companies to voluntarily disclose FCPA-related misconduct. Under the revised policy, when a company voluntarily self-discloses misconduct, fully cooperates, timely and appropriately remediates and agrees to disgorge any ill-gotten profits, there is a presumption that the DOJ will decline to prosecute the company. That presumption will be overcome only if there are aggravating circumstances related to the nature and seriousness of the offense, such as where the company was a repeat offender or where the misconduct was pervasive, involved executive management or resulted in significant corporate profits. Recently, DOJ officials clarified that the FCPA enforcement policy applies when an acquiror unearths FCPA violations in connection with an acquisition, and indicated that they are employing the policy's principles as "non-binding guidance" in corporate investigations outside the FCPA arena.

Meanwhile, commitment to anti-corruption enforcement is on the rise across the globe. Trump Administration officials at the DOJ and the SEC have pledged continued vigorous enforcement of the FCPA, and have brought significant enforcement actions against both individuals and corporations. In countries from Europe to South America to Asia, new anti-corruption laws are taking effect, and enforcement actions are being pursued. And corruption investigations have become increasingly international in nature, with the most significant FCPA resolutions of 2017 involving coordinated international resolutions, where multiple countries imposed penalties and shared penalty proceeds.

Cybersecurity. The EU's General Data Protection Regulation (GDPR), which took effect on May 25, 2018, raises the regulatory bar, and sweeps more broadly than some non-EU-based companies may realize. The GDPR imposes stringent requirements on both data collection and data processing, including increased data security mandates, enhanced obligations to obtain data owner consent, and strict breach notification requirements. Importantly, the GDPR is extraterritorial in its reach, and carries severe penalties for noncompliance—up to 4% of worldwide revenue. In the United States, the New York State Department of Financial Services (DFS) has implemented detailed and prescriptive regulations of its own, requiring covered institutions—entities authorized under New York State banking, insurance or financial services laws—to meet strict minimum cybersecurity standards. The revised regulations require, among other things, that covered institutions have in place a cybersecurity program designed to protect consumers' private data, approved by boards of directors or senior corporate officers and accompanied by annual compliance certifications, the first of which was required to be filed on February 15, 2018. In addition, on April 16, 2018, the National Institute of Standards and Technology (NIST) released an updated version of its Cybersecurity Framework, a critical benchmarking tool used not only by businesses across the globe, but by key regulators like the SEC and the Federal Trade Commission.

Meanwhile, the SEC has turned its attention to market disclosure and breach notification. Since 2011, when the SEC's Division of Corporation Finance issued interpretive guidance regarding cybersecurity disclosures, public companies have been required to "disclose the risk of cyber incidents if they are among the most significant factors that make an investment in the company speculative or risky." In February 2018, the SEC issued new guidance to clarify its expectations as to such disclosures. The majority of the 2018 guidance focuses on "reinforcing and expanding upon" the 2011 guidance, advising public companies to evaluate the materiality of cyber risks and incidents and make necessary disclosures in a timely fashion, while warning that the SEC is watching closely. However, the 2018 guidance delves into some new areas – particularly board oversight, disclosure controls and procedures, insider trading and selective disclosures. As it regards risk oversight, the 2018 guidance advises that public companies should disclose the role of boards in cyber risk management, at least where cyber risks are material to a company's business. Therefore, while most boards are likely already engaged in some form of cyber risk oversight, the call by the SEC for more public disclosure may prompt consideration of whether to deepen or sharpen that engagement.

On the enforcement side, the SEC has adopted a more aggressive approach, engaging in high-profile enforcement actions following its investigations of major data breaches at Yahoo! and Equifax. In April 2018, the SEC announced that Altaba, the entity formerly known as Yahoo!, had agreed to pay a $35 million penalty to settle charges that it misled investors by waiting two years to disclose a data breach in which hackers stole the personal information of more than 500 million Yahoo! users. In its press release announcing the settlement, the SEC explained, "We do not second-guess good faith exercises of judgment about cyber-incident disclosure. But we have also cautioned that a company's response to such an event could be so lacking that an enforcement action would be warranted. This is clearly such a case." While the Yahoo! case should not be read as requiring public disclosure of every data breach, the SEC's action does highlight the need for companies to maintain effective controls and procedures to ensure that internal reports of cyber incidents, or the risk of such incidents, are properly and timely assessed for potential disclosure.

In its February 2018 guidance, the SEC warned that "directors, officers, and other corporate insiders must not trade a public company's securities while in possession of material nonpublic information, which may include knowledge regarding a significant cybersecurity incident experienced by the company." In March and June 2018, the DOJ and SEC filed criminal and civil charges against two former Equifax employees – a chief information officer and a software engineer – for insider trading in advance of the company's September 2017 announcement of a breach that exposed the personal data of approximately 148 million U.S. customers. In light of the government's enhanced focus on the intersection between cybersecurity and insider trading, companies would be wise to examine their insider trading policies to ensure they operate effectively in the wake of cyber incidents, including by ensuring that consideration is given in any specific situation whether to restrict trading by insiders before public disclosure.

Third-Party Guidance on Best Practices

Various industry-specific regulators and private organizations publish suggested best practices for board oversight of risk management. Examples include reports by the National Association of Corporate Directors (NACD)—Blue Ribbon Commission on Risk Governance and the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

In September 2017, COSO released the final version of its updated internationally recognized enterprise risk management framework, which it originally released in 2004. As 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 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. 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.

III. RECOMMENDATIONS FOR IMPROVING RISK OVERSIGHT

As an oversight matter, the board should seek to promote an effective, on-going risk dialogue with management, design the right relationships between the board and its standing committees as to risk oversight and ensure appropriate resources support risk management systems. 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 board and appropriate board committees may consider as part of their risk management oversight include the following:

- review with management the company's risk appetite and risk tolerance and assess whether the company's strategy is consistent with the agreed-upon risk appetite and tolerance for the company;

- 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 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;

- 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, 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 each 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 connection with the above, 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. 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 external events, 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.

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, spinoffs that leave the resulting companies with smaller capitalizations or underinvestment in areas important to the future competitiveness of the company. While actions advocated by activists 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, as well as to explain its decisions to its shareholders.

Situating the Risk Oversight Function

While fundamental risks to the company's business strategy are often discussed at the full board level, most boards continue to delegate primary 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 and matters relating to board and executive succession are often addressed by the nominating and governance 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 2017 Ernst & Young survey of S&P 500 companies, more than 75% of boards have at least one committee in addition to the mandatory committees (audit, compensation and governance), up from 61% in 2013, and of such boards, 11% have a separate risk committee. Separate risk committees remain less common 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).

As noted above, risk management issues may arise in the context of the work of committees other than the committee charged with primary oversight of risk management, and the decision-making by those other 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. 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.

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 among the directors, senior management and other senior risk managers in the company. If directors do not believe they are receiving sufficient information, they should be proactive in asking for more. 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. It may also be appropriate for the committee(s) 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. 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 the company's commitment to full compliance with legal and regulatory requirements, as well as internal policies. 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 DOJ will assess under the Federal Sentencing Guidelines in the event that corporate personnel engage in misconduct. In addition, while Deputy Attorney General Rosenstein has announced a review of all DOJ enforcement guidance memos, including the 2015 "Yates memo" on holding individuals accountable for wrongdoing, we expect that an emphasis on individual accountability will remain a key feature of the enforcement landscape, highlighting the continued importance of companies swiftly and responsibly investigating and remediating 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 to assess their effectiveness and to make any necessary changes. Policies and procedures should fit with business realities. A rulebook that looks good on paper but is not followed will end up hurting rather than helping. 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.

Special Considerations Regarding Cybersecurity Risk

The ever-increasing dependence on technological advances that characterizes all aspects of business and modern life has been accompanied by a rapidly growing threat of cybercrime, the cost of which, according to a 2017 report by Herjavec Group, is expected to grow to more than $6 trillion annually by 2021. As recent examples (*e.g.*, the hacking of computer networks belonging to the SEC

and to Equifax) have highlighted, network security breaches, damage to IT infrastructure and theft of personal data, trade secrets and commercially sensitive information are omnipresent risks that pose a significant financial and reputational threat to companies of all kinds. With computing devices increasingly embedded in everyday items and connected to the "Internet of Things," virtually all company functions across all industries are exposed to cybersecurity risk.

In light of the growing number of successful cyber attacks on even the most technologically sophisticated entities, lawmakers and regulators in the United States and abroad have increased their attention to cybersecurity risk. In the United States, regulatory and enforcement activity relating to cybersecurity has continued to ramp up at the state level. Internationally, the GDPR has significantly increased data handling requirements for companies with even a minimal European nexus. Companies are thus facing a two-front storm, with regulatory risks compounding the security threat.

In response, engaged corporate leaders should implement comprehensive cybersecurity risk mitigation programs, deploying the latest defensive technologies without losing focus on core security procedures like patch installation and employee training, executing data and system testing procedures, implementing effective and regularly exercised cyber incident response plans, and ensuring that the board is engaged in cyber risk oversight.

As cybersecurity risk continues to rise in prominence, so too has the number of companies that have begun to specifically situate cybersecurity and cyber risk within their internal audit function. A recent Internal Audit Capabilities and Needs Survey, conducted by Protiviti, found that 73% of the companies surveyed now include cybersecurity risk as part of their internal audit function, up from 53% in 2015. Directors should assure themselves that their company's internal audit function is performed by individuals who have appropriate technical expertise and sufficient time and resources to devote to cybersecurity risk. Further, the internal audit team should understand and periodically test the company's risk mitigation strategy, and provide timely reports on cybersecurity risk to the board's audit committee.

In satisfying their risk oversight function with respect to cybersecurity, boards should 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.

Special Considerations Regarding ESG Risks

ESG risks represent a specific subset of general risks that a company must manage where relevant, by identifying and mitigating company-specific risks, such as environmental liabilities, labor standards, consumer and product safety and leadership succession, and contingency planning for macro-level risks, including by identifying supply chain and energy alternatives and developing backup recovery plans for climate change and other natural disaster scenarios. While boards have been overseeing management of such material risks for as long as they have existed, increasing scrutiny to ESG issues by the public and some of the largest institutional investors in the world now calls for special attention to be paid to ensuring that the board is satisfied as to how ESG-related risks specifically are being evaluated, disclosed and managed.

Major institutional investors increasingly view ESG issues as having the potential to significantly affect a company's long-term financial value. As stated in a letter by Chairman and CEO of BlackRock, Laurence D. Fink, "In the

current environment . . . stakeholders are demanding that companies exercise leadership on a broader range of issues. And they are right to: a company's ability to manage environmental, social, and governance matters demonstrates the leadership and good governance that is so essential to sustainable growth[.]" BlackRock has further remarked that just as it expects companies to understand the macroeconomic and industry trends in which they operate, it also believes that a company's awareness of ESG-related trends helps drive long-term performance and mitigate risk. For this reason, one of the four main reasons BlackRock will engage with a company is if that company has been identified as lagging its peers on ESG matters that may materially impact long-term economic value. State Street has been a vocal advocate of ESG risk oversight, and in 2016 and 2017 issued a series of frameworks and reports for directors regarding such matters, especially as to integrating sustainability and ESG-related risk matters into corporate strategy. In addition, State Street recently indicated that it intends to enhance its engagement with independent directors on the issue of climate change in order to better understand their views and oversight of the climate-related risks facing their companies. In its 2018 Investment Stewardship Annual Report, Vanguard noted that it looks for "competent boards" that are "educating themselves on sustainability issues," and that it encourages boards to seek out perspectives and information. Vanguard also expects boards to actively evaluate these issues and integrate material sustainability risks into their strategic decision-making.

As the public conversation on the role of companies in addressing environmental and social issues continues to evolve, boards should consider how their risk oversight role specifically applies to ESG-related risk. In large part, the board's function in overseeing management of ESG-related risks, such as supply chain disruptions, energy sources and alternatives, labor practices and environmental impacts involves issue-specific application of the risk oversight practices discussed in this memo. However, due to the fact that the public and investors have increasingly begun to scrutinize how a company addresses ESG issues, the board should ensure that its risk oversight role is satisfied in regards to ESG risk management.

ESG matters often have important public, investor and stakeholder relations dimensions. The board should work with management to identify ESG issues that are pertinent to the business and its customers and decide what policies and processes are appropriate for assessing, monitoring and managing ESG risks. The board should also be comfortable with the company's approach to external reporting of the company's overall approach, response and progress on ESG issues. It is also increasingly important for directors and management who engage with

shareholders to educate themselves and become conversant on the key ESG issues facing the company.

In certain cases, the board may wish to consider receiving regular briefings on relevant ESG matters and the company's approach to handling them. Creating more focused board committees or subcommittees, such as a "corporate responsibility and sustainability" committee, that is specifically tasked with oversight of specified ESG matters or updating existing committee charters and board-level corporate governance guidelines to address the board's approach to such topics may also be considered. Of course, the board should ensure that any committee tasked with ESG risk oversight properly coordinates with any other committees tasked with other types of risk oversight (*i.e.*, the audit committee) so that the board as a whole is satisfied.

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. This includes understanding risks inherent in the company's strategic plans, risks arising from the competitive landscape and the potential for technology and other developments to impact the company's profitability and prospects for sustainable, long-term value creation. 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
Remi P. Korenblit
Monica M. Heinze