DIRECTOR ESSENTIALS

Strengthening Risk Oversight

DIRECTOR ESSENTIALS: STRENGTHENING RISK OVERSIGHT

Purpose of This Report

As the number and magnitude of business risks increase, so do the expectations for stronger risk oversight—through both greater board awareness of risk and more disciplined board review of enterprise risk management (ERM). This report from the National Association of Corporate Directors (NACD) outlines the risk oversight challenge in the current business environment, describes leading risk oversight strategies, and offers tools that all directors can use to oversee risk more effectively.

How Boards Can Use This Resource

- Understand the expectations placed on directors to deliver effective risk oversight.
- Learn about leading practice in risk management and oversight.
- Increase the ability to assess risk and interpret risk reports from management.
- Apply specific tools in the boardroom to effectively engage management on risk-related matters.

1 Navigating Risk in the Current Environment

The International Standards Organization (in ISO 31000) has defined risk as "the effect of uncertainty on objectives," which can be a negative or positive deviation from what is expected.[1] The Committee of Sponsoring Organizations of the Treadway Commission (COSO) currently defines risk as "The possibility that events will occur and affect the achievement of strategy and business objectives."[2] Each kind of risk exposes a company to potential loss; in fact, insurance professionals have defined risk as the possibility of loss.[3] Yet when viewed as part of an active business dynamic, risk—as daunting as its manifestations may be—is far more than the chance of loss. Rather, risk is a level of uncertainty that can create economic opportunity; risks are choices that companies make and individuals take.

In this sense, as many have noted, without risk there is no reward. The capacity to manage risk and the willingness to take risk and make forward-looking choices are key elements that drive growth and position companies to create long-term value. Thus, effective oversight of risk is not about risk elimination: companies win because they do a better job of taking risks, not because they do a better job of avoiding them. And therefore effectively overseeing how risks are chosen and handled becomes an essential board role in stewarding long-term value creation.

Boards and executive teams today are challenged by a fast-changing, highly interdependent, and often ambiguous external environment that is continually creating unforeseen opportunities and risks. In today's business landscape, volatility is the new normal. Businesses are experiencing shortening boom-and-bust business cycles amid growing economic uncertainty. Companies are also operating in an environment of hyper-transparency: business conduct is increasingly visible and scrutinized simultaneously by media, regulators, and shareholders, aided by instantaneous technology. And all this is occurring in a new kind of extended enterprise: the increased use of offshoring, outsourcing, and shared service arrangements have reduced direct management control over risks but not accountability for those same risks. Meanwhile, we are also dealing with information intensity: use of "big data" and increased digitization provides greater analytical capabilities and information advantages, but it also raises the risk of cybersecurity attacks and data privacy breaches—both corporate and customer.[4] Finally, businesses are subject to regulatory proliferation: growth of regulatory demands and enforcements globally and across sectors.

The importance of risk oversight in this environment is not lost on shareholders or their advisors: 2016 voting guidelines by leading proxy advisors highlighted risk oversight as a metric for board performance—an emphasis likely to continue in 2017 and beyond.[5] Respondents to the NACD 2016-2017 Public Company Governance Survey reported that when their boards met with institutional investors in the past year (as half did), nearly 1 in 10 discussed risk management.

It's no surprise therefore that directors are focused on strengthening their risk oversight capabilities. NACD's Public Company Governance Survey also found that more than one in

three respondents said it was "important" or "very important" to make improvements in board oversight of both risk management and cyber risk. When asked to identify areas where the board needed to improve its own expertise, more than 1 in 10 respondents chose risk management expertise.[6] Over the next 12 months, surveyed directors are particularly concerned about the impact of global economic uncertainty, regulatory burden, industry changes, business model disruptions, and cybersecurity threats.[7] (See Sidebar 1.)

Sidebar 1

What Five Trends Do You Foresee Having the Greatest Effect on Your Company Over the Next 12 Months? Respondents could select up to five trends from a list of 16. Bars represent the percentage of respondents selecting a trend. Only the five most widely shared trends are shown.

Source: NACD 2016-2017 Public Company Governance Survey.

2 | Risk Governance: Expectations for Boards

The very concept of oversight implies governance—a system of accountability. At the top of the corporate system, the board is accountable to the corporation as a whole and to its shareholders.[8] Management reports to the board, which oversees them. The Report of the NACD Blue Ribbon Commission on Risk Governance outlined five key categories of board-level risk oversight responsibility. (See Sidebar 2.)

Additional guidance on this point comes from COSO, founded three decades ago and influential in internal control and risk oversight standards since that time.[9] In COSO's proposed 2016 update to its risk oversight standard, it describes this governance system as follows:

> "An entity's governance model defines and establishes authority, responsibility, and accountability. It aligns the roles and responsibilities to the operating model at all levels—from the board of directors to management, to divisions, to operating units, and to functions. Enterprise risk management helps to inform all levels of potential risks to strategy and how the organization is managing them."[10]

In overseeing risk, directors can benefit greatly from the advice of internal and external counsel. They should not journey without these valuable partners. Yet at its heart, board oversight of risk is more a matter of common sense than of law. Although there are no strict legal requirements that identify a comprehensive checklist of the board's risk oversight, there are several risk-related requirements pertaining to public companies and their boards or key committees:

- Companies—All board members must sign the annual report,[11] which includes a Management's Discussion and Analysis of Financial Condition and Results of Operations (MD&A) section that describes "any known trends or uncertainties that have had or that the [company] reasonably expects will have a material … unfavorable impact on net sales or revenues or income from continuing operations."[12]
- Boards—Under "proxy enhancements" effective February 2010, boards must disclose their role in risk oversight.[13]
- Directors (duties of care and loyalty)—Although the corporate director's fiduciary duties of care and loyalty remain general, with no specific reference to risk oversight, it is important to keep both duties in mind. With respect to the duty of care, the landmark decision in Caremark offers some general outlines to consider with respect to information and reporting systems. In Re Caremark International Inc. Derivative Litigation, decided in Delaware Chancery Court in 1996, found that the duty of care requires assurance of reasonably designed corporate information and reporting systems.[14] Regarding the duty of loyalty, it is crucial

SIDEBAR 2 FIVE KEY CATEGORIES OF BOARD-LEVEL RISK OVERSIGHT RESPONSIBILITY

Regardless of industry, organizational strategy, and the unique risks of every organization, the risks and responsibilities facing each board can be broken into the following broad categories:

Governance Risks—Directors are responsible for decisions regarding board leadership and composition, board structure, director selection, CEO selection, and an array of other governance issues critical to the success of the enterprise.

Critical Enterprise Risks—The board needs to be fully engaged to understand the critical risks facing the enterprise, such as technological obsolescence. This may include the top 5 to 10 risks that threaten the company's strategy, business model, or viability—and the status of management's efforts to manage these risks, for which it is responsible.

Board-Approval Risks—The board must approve of decisions regarding major strategic initiatives. Acquisitions, divestitures, major investments, entry into new markets, or new products, etc., require board approval. These may typically be defined in corporate policies.

Business Management Risks—Directors must be knowledgeable of other risks associated with the operations of the business. These risks include day-to-day operations of the business, which the board does not have the time to consider on an individual basis.

Emerging Risks and Non-Traditional Risks—Directors must be knowledgeable about external risks such as demographic shifts, climate change, as well as catastrophic events. Management, however, is responsible for the handling of these risks.

Source: Report of the NACD Blue Ribbon Commission on Risk Governance (NACD, 2009).

to avoid conflicts of interest, real or perceived, when making risk-related decisions and to use disclosure and recusal when appropriate.

- Audit committees—The New York Stock Exchange requires that audit committees "discuss policies with respect to risk assessment and risk management."[15]
- Compensation committees—Under the above-mentioned proxy enhancements, companies must make proxy disclosures if their compensation policies and practices create risks that are "reasonably likely" to have a "material adverse effect" on the company.[16]
- Risk committees—Required under Dodd-Frank, these rules are for bank holding companies with more than $10 billion in assets. In a recent NACD survey of public company directors, 18.9 percent of all respondents (including bank directors, which accounted for less than half of these respondents) said they had a risk committee.[17]

The financial services industry has additional requirements, most notably:

- Banks—As mentioned above, under Dodd-Frank rules, banks with assets over $10 billion are required to have a risk committee, and banks with assets over $50 billion must have chief risk officers (CROs).[18] Furthermore, the Office of the Comptroller of the Currency has published detailed risk oversight guidance for directors of national banks and federal savings associations.[19]
- Broker business continuity plans—The New York Stock Exchange and Nasdaq require that brokers who belong to the exchanges ("members") have business continuity plans.[20] Furthermore, there is a pending U.S. Securities and Exchange Commission (SEC) rule that would extend this requirement to all advisors.[21]
- Insurance companies—The National Association of Insurance Commissioners has a Model #505 policy, which went into effect on January 1, 2015, requiring insurers above a specified premium threshold to maintain a risk management framework, complete its Own Risk and Solvency Assessment (ORSA), and file a confidential annual ORSA Summary Report with its lead state supervisor. All states are expected to adopt Model #505 by the end of 2017.[22] Furthermore, on June 3, 2016, the Federal Reserve Board released a notice of proposed rulemaking to apply enhanced prudential standards to "systemically important" insurance companies.[23]
- Investment companies—In a guidance update published June 2016, the staff of the Division of Investment Management underscores the importance of mitigating operational risks related to significant business disruptions, particularly through proper business continuity planning for registered investment companies.[24]

The above regulatory requirements, as important as they may be, do not help directors actually oversee risk. To oversee risk effectively, directors need to heed examples from successful experience.

In the following section, we outline eight practices—drawn from NACD research and Blue Ribbon Commission and Advisory Council recommendations, and interviews with directors and subject-matter experts—that collectively can help boards strengthen their risk oversight capabilities.

3 Practices for Delivering Effective Risk Oversight

Boards scrutinize many different kinds of risk exposures, and approaches to risk oversight vary widely across industries. Yet, there is a set of common approaches for effective risk oversight that all boards may consider adopting. (See Sidebar 3.) In this section, we outline these practices, emphasize why they matter, and offer practical guidance to implement them.

Sidebar 3
Effective Board Risk Oversight Practices

Practice 1: Clarify the Roles of the Board, Committees, and Management

The board, all board committees, and all members of senior management need to know their unique roles in risk oversight.

Why This Is Important

Without clarity on roles, redundancies and lapses can occur. The practice helps establish a clear mandate for board risk oversight and offers management a blueprint for the execution of risk management.

Potential Red Flags

- There is no mention of "risk" in the board's governance guidelines, committee charters, and/or management job descriptions.
- Management hasn't adopted a formal risk program or structure to address enterprise risks.
- There is no discussion of what risks management should report to the board or board committees or how and when.
- Risk reporting is highly fragmented across committees, preventing the full board from obtaining a single view of risk.

Approach to Consider

Risk oversight is an activity that cannot be reserved for a single corporate officer or a single board committee—whether risk, audit, or another. Rather, it requires the complete and continuous attention and engagement of the full board and the full management team, as well as qualified advisors, all working together.

Boards and their committees may consider adopting several practices for organizing effective oversight and working with management to delineate their respective roles and areas of collaboration:

- Management and the board may consider creating a protocol for their roles in the oversight and management of risk, as described below. (See Sidebar 4.)
- The full board should oversee risks with broad implications for the company's strategic direction, as well as the interplay among various risks. As such, all board members should be knowledgeable about the risk universe in which the company operates and understand how these risks affect strategy, both in the short- and long-term. Results from the most recent NACD public company survey show that the vast majority of respondents put the full board in charge of the big picture for risk oversight. Respondents also agreed on the whole that the full board should be responsible for overseeing "reputational risks," defined as threats to the organization's brand or public standing.[25]
- Each board committee should address risks inherent in its respective areas of oversight (e.g., for the audit committee, financial reporting and internal controls; for the compensation committee, executive compensation; and for the nominating and governance committee, director qualifications).
- Regarding committee oversight of risks, the following pattern emerged from a majority of NACD survey

respondents: audit committee oversees compliance risks, cyber risks, and financial stability risk, while the compensation committee oversees talent risks and incentive risks.[26] Survey results also showed a role for the nominating and governance committee in talent risk (reflecting their role in recruiting board talent and in CEO succession, in some cases). The survey findings did not indicate any dominant role for risk committees, but one purpose for such a committee would be to aggregate and analyze risk for the board and committees.

- Management can maintain continual risk awareness in its plans and operations, reporting regularly on risk to the board. To support its work, management can establish a corporate committee focused on risk, which reports to the board and owns the risk management framework for the organization. Such a committee might have legal, audit, compliance, supply chain, finance, HR, and technology representatives.

SIDEBAR 4 BOARD VERSUS MANAGEMENT ROLES IN RISK OVERSIGHT

The following illustration (recapping points made elsewhere in this report) shows one way to visualize the roles:

Board/committee responsibilities:

- Clarify the respective roles of the full board and standing committees with respect to risk oversight in the board's governance guidelines and committee charters, including those responsibilities that are required by SEC and/or listing exchanges.
- Work with management to understand and calibrate the company's risk profile, risk appetite, and risk program.
- Hold ongoing discussions with management about the risks and assumptions related to strategic choices and associated implementation plans.
- Ensure management has an effective risk management program.
- Ensure that management's risk management program is appropriately resourced.
- Set clear expectations with management about the risk-related information (including content, format, and level of detail) required by the full board and key committees.
- Assess the board's risk oversight activities and processes regularly, as part of executive session discussions and/or board evaluations.
- Monitor progress against the risk mitigation.

Management responsibilities:

- Define the company's risk profile and risk appetite, working with the board to focus on key risks inherent in the corporate strategy/business model.
- Support the work of the board through an internal management committee focused on risk.
- Build and sustain a risk management program to identify, assess, mitigate, monitor, and communicate risk.
- Identify and disclose key risks to the board.
- Ascertain likelihood and significance of risks.
- Mitigate risks.

Practice 2: Understand the Company's Risk Profile

All board members should be aware of the company's key risk exposures, or "risk profile." The glossary that accompanies ISO 31000 defines risk profile as a "description of any set of risks," which can contain those that "relate to the whole organization, part of the organization, or as otherwise defined."[27] The board's focus will be on critical enterprise risks, rather than the risks that arise in the normal course of business operations. As emphasized in the Report of the NACD Blue Ribbon Commission on Risk Governance, it is important to understand the company's key drivers and to assess the risk in the company's strategy.[28]

Why This Is Important

Oversight of any business requires understanding the major risks that it faces now and in the future, and making decisions accordingly. Although the company's "risk universe" may be almost limitless, a company's risk profile is the composite (and analysis) of the most important risks the company faces—risks that impact strategy and reputation. A risk profile identifies and assesses major risks inherent in the company's strategy and business model.

Potential Red Flags

- The company does not have a documented risk profile, or it does not regularly update its risk profile to include emerging risks.
- The risk profile lists enterprise-level risks but does not prioritize them, or the criteria for defining the likelihood and impact of risks is ambiguous.
- The risk profile lists only known short-term risks, not emerging or long-term risks, or the risk profile is largely disconnected from the company's (changing) strategy.
- The risk profile almost entirely relies on internal inputs, or it gives limited consideration to external industry, market, or economic factors.

Approach to Consider

Directors should periodically review the company's risk profile or urge development of one, if it is lacking. Specifically, the full board or audit committee may consider meeting with the head of audit and risk at the beginning of each calendar year to establish the company's risk profile and approve audit and risk mitigation plans against critical risks. To ensure correct risk prioritization, a board can perform in-depth reviews of specific top risks, assessing how they affect corporate value drivers and core business objectives.

When reviewing the risk profile, it is critical to account for the context in which the company operates. For example, examining M&A-related risk would be a high priority for a company that is considering making acquisitions or that is vulnerable to being a target.[29] Or for another example, exchange rate risk is obviously more important to a global player than to a domestic one. Also, the board should be sure to anticipate the future—not just the short-term but also over-the-horizon "sleeper" risks.

Practice 3: Define the Company's Risk Appetite

Boards need to help shape the company's accepted risk appetite and ensure that senior management applies it appropriately throughout the organization. According to ISO 31000, risk appetite is "the amount and type of risk that an organization is prepared to pursue, retain, or take in pursuit of its strategic objectives."[30] Its purpose is to develop a consensus among the board and senior management on what risks (what type and how much) the company is willing to take, and it can be used to set risk management expectations both internally and externally in areas such as capital allocation, major investments, and acquisitions. For example, a company may define formally that it has low appetite for risks that could lead to significant earnings per share volatility.

Companies can check their risk appetite against a risk scorecard. As described in the 2015 proxy statement for the Toronto-Dominion Bank:

> "Risk Appetite: The bank's strategy incorporates a disciplined approach to risk management which is reflected in the board approved risk appetite framework. The committee believes that it is important to consider risk outcomes during the year when determining compensation awards. To facilitate the committee's consideration of risk outcomes at year-end, the CRO presents an enterprise risk scorecard to the risk and human resources committees. This scorecard assesses the enterprise and business unit performance against the bank's risk appetite. Risk adjustments can only be used to reduce the business performance factor, and there is no limit on potential reductions. Thus, incentive awards (including both cash and equity) may be reduced to zero."[31]

Why This Is Important

Companies take risks in order to grow and compete in the marketplace, yet they need guardrails for how much risk they are willing to accept. And the board plays a critical role in defining these guardrails.

Potential Red Flags

- Companies do not use risk appetite frameworks to inform key decisions.
- Managers and teams seem oblivious to key risks; no one seems to be making risk-informed decisions.
- The risk appetite framework is not driven down into the organization, and risk thresholds are not built into key performance indicators.
- The company's risk appetite remains static instead of adapting to changing business needs.

Approach to Consider

To define a company's risk appetite, management and the board need to determine the levels of risk the company is willing to take in various aspects of the business, with some being more risk averse than others.

The following risk appetite statement from a healthcare provider offers a concrete example:

> "The Organization operates within a low overall risk range. The Organization's lowest risk appetite relates to safety and compliance objectives, including employee

health and safety, with a marginally higher risk appetite towards its strategic, reporting, and operations objectives. This means that reducing to reasonably practicable levels the risks originating from various medical systems, products, equipment, and our work environment, and meeting our legal obligations will take priority over other business objectives."[32]

Practice 4: Integrate Strategy, Risk, and Performance Discussions

Every strategic choice entails risk and enables performance; the effective board understands the connections among these three.

Why This Is Important

Heightened environmental uncertainty has placed a greater premium on the use of effective risk management in the formulation and execution of corporate strategy. All too often, risk assessment is completely divorced from the strategy process in the organization, increasing the likelihood of poor, costly decisions.

Potential Red Flags

- Strategy conversations with management lack a rigorous examination of the validity of underlying assumptions and fail to consider different risk scenarios.
- Only the audit committee, and not the full board, reviews risks.
- The full board's projected impact on strategy and business objectives is not measured quantitatively or qualitatively.
- Discussions of strategy, risk, and performance are held as separate events, without cross-reference among the three.

Approach to Consider

Wherever possible, executives reporting to the board should integrate risk reporting with strategy execution and performance reporting. Similarly, the board should ensure that risk discussions are interwoven with strategy and performance. During the planning cycle, boards should expect from management that discussion about next year's corporate objectives will focus on the drivers of value-creation and the top risks affecting those drivers.

Practice 5: Ensure Transparent and Dynamic Risk Reporting

Risk reporting must reach the right people with the right information. It should not be limited to the metrics mandated by external disclosure rules. And it should include all the information the board needs to assess the company's risk exposure. Similarly, reporting should be dynamic, taking into consideration the velocity by which existing risks change or new risks emerge.

Why This Is Important

Aside from the intrinsic value of an uninterrupted flow of information that offers the board a clear view of risk, there is also a legal aspect. As mentioned earlier, reporting is a key aspect of risk oversight. In his classic Caremark decision, Chancellor William T. Allen found that a board cannot meet its duty to be reasonably informed, "without assuring that information and reporting systems exist in the organization that are reasonably designed to provide to senior management and the board, each within its scope, information that will enable them to reach informed judgments concerning both the corporation's compliance with law and its business performance."[33] Outside the company, the board is responsible for certain risk-related disclosures to shareholders. These facts make risk reporting of special importance to directors.

Potential Red Flags

- The board does not have enough time to review the company's mandated disclosures about risks.
- Rankings are delivered annually, but no action is taken—also called enterprise "list" management.
- Static risk heat maps are used, but they do not clarify how exposure to specific risks has changed year-over-year.
- Risk calculations/ratings are based on last year's risk events, business developments, or financial performance, which may lead management and the board to undervalue new trends.

Approach to Consider

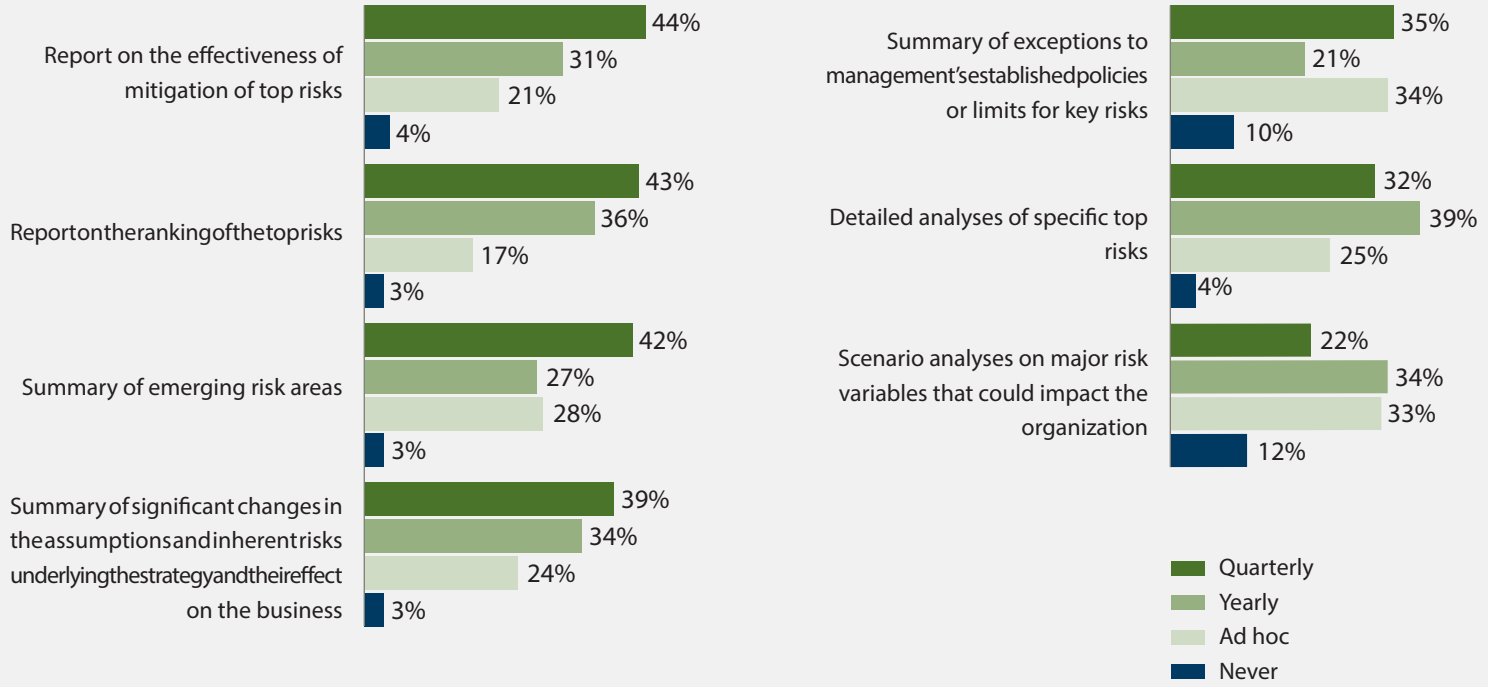
Ensure Validity and Relevance of Risk Reporting:

1. To reduce subjectivity and variability in risk reporting, ask management to clearly define how significant a "high risk" is, how much difference there is between a "high" risk and a "low" risk, and what the difference is between one "high" risk and another. Risk scorecards can be used to track the status of critical enterprise risks, linked to the company's risk appetite.
2. Make sure that the time horizons used to assess the likelihood of risks are consistent with the time horizon of associated business objectives. For example, the risk is seen as likely to occur within the time horizon contemplated by the objective.
3. Understand the velocity and duration of risks. As the current environment has shown, risk velocity—or how quickly a risk's results will manifest if it comes to pass—is an important factor in risk rating. Furthermore, the relative duration of a risk (if it comes to pass, how long will it impact a company?)—for example, a

regulatory or macroeconomic risk—is an important dimension.

4. Ensure two-way information flow, both top-down and bottom-up. It's important to communicate with management about the types of risk information the board requires. Companies need strong escalation processes for critical risks. A good risk reporting system will deter the need for formal whistleblowing—whether the bottom-to-top process mandated by Sarbanes-Oxley or the director regulatory contact incentivized by Dodd-Frank.
5. Make sure there's a regular cadence of risk reporting, allowing the board to frequently assess changes in risk exposure and keep a pulse on the effectiveness of risk management. The NACD 2016-2017 Public Company Governance Survey benchmarks show both frequency and the topical treatment of risk reporting. (See Sidebar 5.)

SIDEBAR 5 HOW FREQUENTLY DOES YOUR BOARD RECEIVE THE FOLLOWING TYPES OF RISK INFORMATION FROM MANAGEMENT?



Source: NACD 2016-2017 Public Company Governance Survey.

Practice 6: Reinforce Clear Accountability for Risk

Why This Is Important

The management of risk in today's often-extended enterprise is complex, with executive teams typically feeling the need to transfer ownership of risks to specialist risk, compliance, and security functions inside the organization or to outsource them to external advisors. However, examination of recent risk disasters reveals that diffused accountability for risk management is a major problem.

Potential Red Flags

- Top enterprise risks lack specific business owners, for both risk monitoring and risk mitigation.
- Risk management effectiveness goals and ownership for specific business risks are missing in senior management performance expectations and incentive plans.
- Nobody in the organization is held directly accountable for controllable risk failures.
- Accumulation of specialist risk functions and staff at headquarters may lead profit and loss owners to ignore their ownership for risks.

Approach to Consider

Make sure that management has built a robust internal risk governance model, with authority, responsibility, and accountability clearly delineated across the business and its support functions, including internal audit, legal, compliance, ERM, sustainability (e.g., environmental, health, and safety issues), and information security. When drilling down on specific risks and their mitigation, ensure that formal accountability is assigned at the executive level and that funding can be allocated to treat the risk.

One commonly used model for risk ownership asserts three lines of defense. In this model, the first line of defense is management (a function that owns and manages risk), the second line is risk control and compliance oversight (management-level functions that oversee risks), and the third is the function that provides independent assurance, such as internal audit.[34] Heavily regulated sectors (e.g., financial services) have a fourth line of defense: regulators (e.g., bank supervisors).[35]

Practice 7: Verify That Mitigation Reduces Risk Exposure

Why This Is Important

The success or failure of risk mitigation is often underreported, leaving boards with a limited understanding of whether or not risks are effectively minimized over time.

Potential Red Flags

- Risk mitigation is delayed or watered down due to funding constraints or competing priorities.
- Management has not defined how its operations will effectively mitigate risk or what a well-controlled risk should look like.
- There is an increase in the number of risk surprises, including near-misses and incidents, despite risk mitigation measures.
- Human and process breakdowns or errors continue in specific risk areas despite mitigation, such as policies or training, being enacted.
- Internal audit and management have significantly different views about the measures required to address a risk.

Approach to Consider

Ask management to report mitigation success metrics for top enterprise risks, including key indicators such as reduced process or control breakdowns or changes in employee behavior over time. The audit committee would be wise to get a sense of all three lines of defense:

- First, this means receiving reports from those who lead the functions where risk resides (the front line, or first line of defense). For example, if supply chain risks have been identified as critical to the company, the board would receive reports from the head of procurement.
- Second, being risk aware also means meeting with the senior officer in charge of risk oversight, such as the CRO, the chief compliance officer, and/or the chief information security officer.
- Third, the head of internal audit serves as a third line of defense.

By building awareness of all three lines of defense, audit committee members can better understand whether the organization is truly committed, in terms of funding and goal setting, to remediating critical risks. COSO has noted that ERM helps a company manage risks to reduce the likelihood that an event will occur and to manage the impact when one does occur. Managing the impact, notes COSO, may include implementing a "crisis management plan."[36]

Practice 8: Assess Risk Culture

Risk oversight requires understanding the company's "risk culture." One useful definition of this term comes from a recent Oliver Wyman report that defines risk culture as "the behavioral norms of a company's personnel with regard to the risks presented by strategy execution and business operations."[37]

A weak risk culture, says Oliver Wyman, shows a "high degree of fragmentation with respect to expected behaviors and a low level of accountability for decisions and actions."[38] In contrast, a strong culture will show a unified approach to risk and a high degree of accountability for it. There will be continuous process improvement.

Additionally, the NACD Advisory Council on Risk Oversight—a group made up of risk and audit committee chairs of Fortune 500 companies—recently discussed the board's role in the oversight of risk culture, emphasizing the importance of prudent risk taking as the core element of a strong risk culture. (See the Additional Risk Oversight Resources at the end of this report.) Boards should frequently assess whether their companies are well positioned through their people to take the right risks while avoiding undue risks.

Why This Is Important

Culture is often described as how work really gets done when no one is looking, and it is critical to ensuring a successful and sustainable strategy. A strong culture can fuel employee engagement, unleash innovation, and deter fraud and abuse.

Potential Red Flags

- There is a sense that senior managers "fear" the CEO or that the company will retaliate against the messenger of bad news.
- Consistently poor employee engagement data (often in specific pockets of the organization) is drawn from surveys or exit interviews.
- Senior management tolerates misbehavior from top performers and does not consistently penalize offenders of the code of conduct.
- There is a disconnect between what the company reports on risk and how people really behave to achieve business objectives.
- A strong tone at the top has not spread to the middle management and operational levels of the company.
- Incentive plans reward behaviors that defy the company's stated values and create the potential for excessive risk taking.

Approach to Consider

To influence and assess risk culture, the board can use a number of important levers:

1. Incentivize the right behaviors by designing appropriate compensation plans and targets.

2. Assess what the real culture is; look at relevant indicators, review employee surveys, and conduct site visits. Are employees comfortable speaking up about problems?
3. Select and evaluate senior leaders based on a commitment and proven track record in building and maintaining a strong culture.
4. Set the right example in your boardroom culture by allowing concerns and dissent to surface, and by making it "safe" for management to express uncertainty or doubt.

4 Board Risk Oversight Questionnaire

For each of the risk oversight practices, we have identified key questions to help drive dialogue with management and obtain a robust understanding of the effectiveness of risk management activities throughout the organization. This list incorporates questions from the Report of the NACD Blue Ribbon Commission on Risk Governance.[39]

Clarify the Roles of the Board, Committees, and Management

- Is there a common understanding among management, the board, and board committees about their respective roles, responsibilities, and accountabilities on strategy? For example, is the board and are the appropriate committees meeting regularly with a CRO? If there is a CRO, has the board ensured that the CRO and general counsel have adequate resources and appropriate reporting lines to bring any changes in material risks to the board's attention?
- Are risk oversight activities clearly differentiated between the board and its committees, and among the various committees?
- Does the board have the appropriate committee structure for its significant oversight obligations in the risk area?
- How specifically are our board committees engaged in risk oversight? For example, how is our audit and/or risk committee discussing risk controls, risk assessment policies, and risk management polices?[40] How does the compensation committee evaluate potential risks in executive pay plans and in the company's pay philosophy overall?
- How does the nominating and governance committee factor risk and strategy considerations into board succession planning and director recruitment needs?
- What is the threshold for risk-related reporting to the board (e.g., categories of risk, specific issues or incidents)? What situations may call for greater board engagement (e.g., perceived management failure to disclose or address a critical risk)? Do we have a protocol that defines these situations?

Understand the Company's Risk Profile

- What are the strategic assets we must protect at any cost?
- Is our risk profile clearly aligned with the company's key value drivers and strategy?
- What negative events could occur that would harm our core assets?
- Have we sufficiently considered risks that we could be indirectly exposed to, for example, via our supply chain, vendors, customers, or elsewhere in our corporate ecosystem?
- How does management measure the likelihood, severity, and velocity of individual risks?

- How do we compare to our peers (e.g., benchmarks for incident levels, regulatory audits)?

Define the Company's Risk Appetite

- Given our risk profile and our strategy, what risk appetite should we have? Have we clearly cascaded our risk appetite into operational-level decision-making processes?
- Do the board and committees discuss risk appetite with management?
- How can this discussion become a part of the board's regular routine?
- Are we too cautious? How so? Are we too reckless? How so?
- What signals is the investment community sending about our willingness to take risks?
- Are the risks we are willing to take commensurate with the rewards we seek?

Integrate Strategy, Risk, and Performance Discussions

- When we discuss strategy, how do we consider risks?
- To what extent is there a consensus among directors about the risks related to the company's (future) strategy? If there are different perspectives among directors, how are those handled? Do the board committees share information about risks they have individually reviewed and discussed?
- How do we as a board evaluate whether our strategy itself is too risky or risk averse? How frequently do we conduct this assessment?
- What capabilities are required to address risks, and do our hiring goals and job performance metrics reflect these? Where do we have capability gaps?
- Has the board and have the appropriate committees reviewed the incentive structure with strategy and risks in mind?
- Has the board and have the appropriate committees reviewed board composition and director skill sets in relation to up-to-date competencies for oversight of the company's strategy, business lines, and material risks?

Ensure Transparent and Dynamic Risk Reporting

- Do the directors receive risk material that adequately distills vast quantities of risk information into prioritized, actionable summaries?
- Have we achieved a common understanding of what triggers bring an issue to the board's attention? Has management developed key risk indicators that offer early warnings into increased exposure? What is the threshold, and the process, for reporting to the board about sudden changes to the company's risk profile?
- Does management offer clear definitions about the likelihood and impact of risks, including both quantitative and qualitative dimensions? When the financial reports show losses, how do these compare to the risks that have been identified? Are the losses (if any) consistent in magnitude and frequency with what one could expect given the risk profile presented to the board?
- Do risk reports demonstrate the relationships or interdependencies between specific individual risks?
- Do risk reports cover all types of risk exposures,

including those that are strategic, operational, compliance-related, and IT-related? Are the risks associated with business units presented to the board in a comprehensive, holistic manner?

- Does intelligence about emerging risks effectively escalate from the front lines of the organization to the top?

Reinforce Clear Accountability for Risk

- Is accountability for top risks formally assigned to members of the senior executive team? How is this accountability cascaded through the organization?
- Does accountability for risks come with budgetary authority to devote sufficient resources to risk mitigation and implement necessary controls? Does the board have sufficient personnel (including advisors) and financial resources in place to enable it to fulfill its risk engagement responsibilities?
- Does the board have a clear understanding of where strategy and risk oversight are delegated and what processes are used within management and among business units?
- Which individuals are accountable for monitoring indicators related to the company's key risks? Where do they sit in the organization in terms of seniority?
- As we reward our managers, do we take into account their ability to anticipate and manage risk? Is accountability/performance around risk effectively embedded in incentive structures at all levels of the organization? How far down the reporting chain do our incentives for risk management excellence go?

Verify That Mitigation Reduces Risk Exposure

- Do we clearly differentiate between risks that can and cannot be mitigated?
- Are our mitigation plans realistic? Do we understand that mitigation does not mean elimination?
- Does management have a good understanding of when a risk is effectively mitigated?
- Is internal audit satisfied with management's commitment and discipline in mitigating risks?
- Does management regularly communicate about the success or failure of risk mitigation?
- Did we see any surprise risks over the past 12 months that should have been mitigated?

Assess Risk Culture

- Are we confident that senior management generally agrees on strategy and its risks? Or if not, is the board learning about disagreements—that is, has management been forthcoming about any differences among senior leadership regarding material strategic recommendations and decisions?
- Do we have a culture in which staff at all levels know what risks to take and what risks to avoid?
- How willing are employees to speak up about problems that can cause significant risk to the organization?
- How do the compensation structure and performance goals we have set for the executive team prevent excessive risk-taking behaviors at multiple levels of the organization?

- What information does the board receive about the tone at the middle levels and the front lines of the organization?
- Is there enough trust established between a) the board and the executive team and b) the executive team and middle management to have candid discussions about risks?

5 | Additional Risk Oversight Resources

General Resources

Board Resource Centers on Risk Oversight and Cyber-Risk Oversight
These online resource centers bring together current NACD content, services, and events related to risk oversight. Here you will find practical guidance, tools, and analyses tailored to the full board, relevant committees, and individual directors.

Report of the NACD Blue Ribbon Commission on Risk Governance: Balancing Risk and Reward (2009)
This NACD Blue Ribbon Commission report is a guide for boards to improve their risk management oversight processes. The report includes 10 principles for effective risk oversight and sample risk governance documents, including risk reports and committee charters.

The View of ERM from E*Trade's Risk Chair by James Lam (NACD Directorship, September-October 2016)
Get an inside view of the effective risk oversight program at E*Trade.

Global Risks Report 2016 (World Economic Forum)
This report features perspectives from nearly 750 experts on the likelihood and impact of 29 significant global risks—economic, environmental, geopolitical, societal, and technological—over the next 10 years.

The State of Risk Oversight Report: An Overview of Enterprise Risk Management Practices (NC State/AICPA 2016)
NC State's ERM Initiative, in partnership with the American Institute of Certified Public Accountants, reports here on survey responses from 441 business executives spanning a number of industries and types and sizes of organizations. The seventh in an annual series, the report provides detailed insights about the maturity of their organization's current ERM practices.

Calibrating Risk Oversight (KPMG's Global Boardroom Insights, October 2016)
Get a global view of risk oversight.

Risk Roles

Staying Engaged in Risk Oversight Practice by Jim DeLoach (NACD Directorship May-June 2016)
How can the board ensure that the risk oversight process remains effective over time and engaged with its risk oversight responsibilities?

Who Is Responsible for Risk? (Pearl Meyer, 2015)
Risk oversight has climbed to the top of the boardroom priority list.

The Path Forward: How CROs and CCOs Can Lead (PwC, 2016)
Review insights from in-depth interviews with CROs, chief compliance officers, audit committee executives, and other members of the C-suite.

Risk Appetite

Risk Appetite Frameworks – Considerations for Directors (NACD 2016)
Review Appendix C from the Report of the NACD Blue Ribbon Commission on Long-Term Value Creation.

Sample Risk Appetite Statement (Marsh & McLennan Companies, 2013)
ReviewMMC'sdetailedriskappetitestatementcoveringstrategy, finances, client relations, people, and operating environment.

Risk Appetite Statements (NACD Board Vision, 2014)
Watchavideointerviewaboutriskappetitestatementsfeaturing perspectives from NACD and Marsh & McLennan.

Risk, Strategy, and Performance

What Is Enterprise Risk Management? (2016 Report by Professor Mark Beasley)
"Theobjectiveofenterpriseriskmanagementistodevelopaholistic,portfolioviewofthemostsignificantriskstotheachievement of the entity's most important objectives. The 'e' in ERM signals that ERM seeks to create a top-down, enterprise view of all the significant risks that might impact the business. In other words, ERM attempts to create a basket of all types of risks that might haveanimpact—bothpositivelyandnegatively—ontheviability of the business." Beasley, 2016

Risk Reporting

Communicating the Board's Role in Risk Oversight to Investors (NACD Advisory Council on Risk Oversight, 2015)
Investors want to see evidence of a holistic approach to risk oversight. Context matters as much as content.

Emerging Risks: Looking Around the Corner by Jim DeLoach (May 16, 2016)
Anexperiencedconsultantgivespracticaladviceonhoworganizations should identify and communicate emerging risks.

Risk Accountability

COSO Enterprise Risk Management–Integrated Framework (2016 Draft)
ThismostrecentCOSOguidanceisdesignedtohelporganizations "improvetheirapproachtomanagementofnewandexistingrisks as a way to help create, preserve, sustain, and realize value." A revised version will be released in 2017.

COSO ERM Revised: A Commentary by Jim DeLoach (July 28, 2016)
A risk consultant summarizes the revised framework for ERM.

Risk Culture

Advisory Council on Risk Oversight: The Board's Role in the Oversight of Risk Culture
The NACD Advisory Council on Risk Oversight convened in April 2016todiscusstheboard'sroleintheoversightofriskculture.The meeting,cohostedbyPwCandSidleyAustin,highlightedanumber of takeaways for directors, from the importance of prudent risk taking to the traits of a positive risk culture.

NACD Director Dialogue: Board Oversight of Reputational Risk (2015)
Reputation can make or break a brand or a company. With this in mind, NACD and Protiviti convened a series of three roundtable meetings with over 60 U.S. corporate directors in 2014 to discuss how boards can more effectively oversee reputational risk.

NOTES

1 ISO 31000: Risk Management.

2 COSO, "Enterprise Risk Management: Aligning Risk with Strategy and Performance," June 2016.

3 Insurance is defined as a "method of coping with risk. Its primary function is to substitute certainty for uncertainty as regards the economic cost of loss-producing events." "Insurance," by Mark Richard Greene, Encyclopedia Britannica.

4 See NACD, "Cyber-Risk Oversight Handbook," 2014. NACD, in conjunction with AIG and the Internet Security Alliance, has identified five steps that all corporate boards should consider as they seek to enhance their oversight of cyber risks. It includes a sample cyber-risk report. See also Sidley Austin, "Cyber Risk and Insurance," 2015.

5 ISS and Glass Lewis Updated 2016 Voting Policies.

6 Source: Preliminary results from the NACD 2016-2017 Public Company Governance Survey.

7 Preliminary results from the NACD 2016-2017 Public Company Governance Survey found these risks to be top of mind out of 16 choices. For both one-year and five-year trends, the following five issues were identified as a "top five" risk by at least one-third of all respondents. No other risks ranked this highly: 1) global economic uncertainty, 2) increased regulatory burden, 3) significant industry challenges, 4) business model disruptions, and 5) cybersecurity threats. When asked the same question concerning the "next five years," the same five issues rose to the top, but with "significant industry challenges" and "global economic uncertainty" swapping places to become #1 and #3, respectively. Source: NACD 2016-2017 Public Company Governance Survey.

8 For a general guide to director duties, see Corporate Director's Guidebook, Sixth Edition (American Bar Association, 2012). For more details, see also NACD, "Customizable Director Role Description," 2016.

9 COSO's standard for internal control, first published in 1992 and later updated in 2013, has been the basis for the standards set forth by the American Institute of Certified Public Accountants as well as the SEC, which cited the standard Sarbanes-Oxley. (For this history, see Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports.) Furthermore, COSO's standard for ERM, first published in 2004 and now updated for 2016, has also been influential. The SEC cited it in its recently proposed rule that would require ERM for all advisors, per note 21.

10 Op. cit., note 2.

11 The SEC specifies that Form 10-K must be signed "by the registrant, and on behalf of the registrant by its principal executive officer or officers, its principal financial officer or officers, its controller or principal accounting officer, and by at least the majority of the board of directors or persons performing similar functions."

[12] S-K Item 303(a) includes "MD&A" of the company's "financial condition, changes in financial condition and results of operations." And S-K Item 303(a)(3)(ii) indicates that the MD&A must include a description of "any known trends or uncertainties that have had or that the [company] reasonably expects will have a material … unfavorable impact on net sales or revenues or income from continuing operations." Thus, the MD&A has become a kind of master list of risks.

[13] Under Proxy Disclosure Enhancements effective February 28, 2010, a company proxy statement must describe the board's role in the oversight of risk.

[14] See In Re Caremark International, Inc., Derivative Litigation (1996).

[15] Section 303A, NYSE Listing Manual.

[16] Under Proxy Disclosure Enhancements, a company must make disclosures in its proxy statement if the compensation policies and practices create risks that are "reasonably likely" to have a "material adverse effect" on the company.

[17] Source: Preliminary results from the NACD 2016-2017 Public Company Governance Survey, p. 4. Of respondents, 7.8 percent were from banks.

[18] Enhanced Prudential Standards for Bank Holding Companies and Foreign Banking Organizations: Final Rule, March 27, 2014.

[19] Office of the Comptroller of the Currency, "The Director's Book: Role of Directors for National Banks and Federal Savings Associations," July 2016.

[20] SEC, "SEC Approves NASD and NYSE Business Continuity Rules," April 6, 2004; see also SEC, Release No. 34-49537, April 7, 2004.

[21] Adviser Business Continuity and Transition Plans proposed.

[22] National Association of Insurance Commissioners, "Enterprise Risk Management," April 29, 2016.

[23] On June 3, 2016, the Federal Reserve Board of Governors released a notice of proposed rulemaking to apply enhanced prudential standards to systemically important insurance companies. Board of Governors of the Federal Reserve System, Press Release, June 3, 2016.

[24] SEC, "Guidance Update: Business Continuity Planning for Registered Investment Companies," June 2016.

[25] NACD 2016-2017 Public Company Governance Survey.

[26] Op. cit., note 26.

[27] Op. cit., note 1.

[28] These are the first two of 10 principles articulated in that report, Report of the NACD Blue Ribbon Commission on Risk Governance: Balancing Risk and Reward (NACD, 2009), cited in Sidebar 2.

[29] See NACD, "Advisory Council on Risk Oversight: M&A and Transaction Risk Oversight," 2015.

[30] Op. cit., note 1.

[31] Toronto-Dominion Bank 2015 Proxy Statement.

[32] COSO's Enterprise Risk Management-Understanding and Communicating Risk Appetite, January 2012, cited in "Board Oversight of Risk: Defining Risk Appetite in Plain English" (PwC, January 2014).

[33] Op. cit., note 14.

[34] The IIA, IIA Position Paper: The Three Lines of Defense in Effective Risk Management and Control, 2013.

[35] For a discussion from the Bank of International Settlements, see http://www.bis.org/fsi/fsipapers11.pdf.

[36] Op. cit., note 2.

[37] Oliver Wyman, "Risk Culture."

[38] Ibid.

[39] Op. cit., note 28.

[40] Op. cit., note 15.

