Director Notes

THE CONFERENCE BOARD GOVERNANCE CENTER®

Risk Oversight: Evolving Expectations for Boards

by Parveen P. Gupta and Tim J. Leech

This report discusses evolving expectations for board oversight of management's risk appetite and tolerance and the challenges boards face in meeting them. It also recommends steps to implement a board-driven, objective-centric approach to risk governance.[1]

Following the financial crisis, the regulators and elected government officials responsible for ensuring the safety and stability of the global capital markets launched a plethora of commissions and special inquiries aimed at determining why corporate risk management processes had failed. What follows is a summary of the findings of those inquiries and the resulting recommendations by various groups to assess and increase the effectiveness of board oversight of risk. We then discuss the challenges boards typically face in effectively carrying out their risk oversight duties and recommend eight steps for implementing a board-driven, objective-centric approach.

Senior Supervisors Group (SSG) One of most comprehensive and in-depth evaluations of risk management practices was undertaken by the highly influential SSG, a forum composed of financial regulators from Canada, France, Germany, Japan, Switzerland, the United Kingdom, and the United States. The SSG published two reports examining how weaknesses in risk management and internal controls contributed to industry distress during the financial crisis.[2] In an October 21, 2009, transmittal letter accompanying the second report, the SSG highlighted areas of weakness that required further work by financial firms:

- the failure of some boards of directors and senior managers to establish, measure, and adhere to a level of risk acceptable to the firm;
- compensation programs that conflicted with the control objectives of the firm;
- inadequate and often fragmented technological infrastructures that hindered effective risk identification and measurement; and
- institutional arrangements that conferred status and influence on risk takers at the expense of independent risk managers and control personnel.

No. DN-V6N1
JANUARY 2014
Subscribe for free at www.conference-board.org/directornotes

THE CONFERENCE BOARD
Trusted Insights for Business Worldwide

The conclusions of the SSG led to calls from regulators such as the US Federal Reserve and the Financial Stability Board (FSB) for a significant increase in the involvement of boards of directors in risk governance, and specifically in overseeing management's risk appetite and tolerance.[3]

The National Association of Corporate Directors (NACD) Shortly after the 2008 global financial crisis began, the NACD assembled a Blue Ribbon Commission to consider the board's role in risk oversight. The result was a 2009 report, *Risk Governance: Balancing Risk and Return,* which included six key recommendations. While acknowledging that risk oversight objectives may vary from company to company, the report recommended that every board be certain that:[4]

1. the risk appetite implicit in the company's business model, strategy, and execution is appropriate;
2. the expected risks are commensurate with the expected rewards;
3. the management has implemented a system to manage, monitor, and mitigate risk, and that system is appropriate given the company's business model and strategy;
4. the risk management system informs the board of the major risks facing the company;
5. an appropriate culture of risk awareness exists throughout the organization; and
6. there is recognition that management of risk is essential to the successful execution of the company's strategy.

The Conference Board In 2009, The Conference Board published a research report to provide guidance to the members of The Conference Board Directors' Institute on how to approach their oversight responsibilities. Discussing the board's role in risk management, the report noted:[5]

> It is the responsibility of the corporate board to oversee the company's risk exposure. This duty is inherent in the role that boards of directors perform in determining a business strategy that generates long-term shareholder value…the need for boards to oversee the implementation of a top-down and enterprise-wide risk management process may be inferred from the provisions of the Sarbanes-Oxley Act of 2002…as well as the rules included in the new Federal Sentencing Guidelines of 2004 promoting the adoption of well-functioning and qualifying compliance programs.

US Securities and Exchange Commission (SEC) In response to the recommendations of the SSG, the SEC adopted rules requiring enhanced proxy disclosure by all US listed public companies. The new rules state that "… disclosure about the board's involvement in the oversight of the risk management process should provide important information to investors about how a company perceives the role of its board and the relationship between the board and senior management in managing the material risks facing the company. This disclosure requirement gives companies the flexibility to describe how the board administers its risk oversight function, such as through the whole board, or through a separate risk committee or the audit committee, for example."[6]

In a February 2013 statement, SEC Commissioner Luis Aguilar stressed the importance of providing robust disclosure about board oversight of a company's risk management framework as required under Item 407(h) of Regulation S-K:

> Given the magnitude of [the financial] crisis…it would be difficult to overemphasize the importance that investors place on questions of risk management. Has the board set limits on the amounts and types of risk that the company may incur? How often does the board review the company's risk management policies? Do risk managers have direct access to the board? What specific skills or experience in managing risk do board members have? Issuers that offer boilerplate in lieu of a thoughtful analysis of questions such as these have not fully complied with our proxy rules and are missing an important opportunity to engage with investors.[7]

Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) To improve risk oversight among the largest global financial institutions following the 2008 financial crisis, the US Congress enacted the Dodd-Frank Act, which, among other things, requires certain public companies subject to Federal Reserve jurisdiction to establish a board-level risk committee that is responsible for the oversight of a company's enterprise-wide risk management practices.[8]

International Corporate Governance Network (ICGN) The ICGN, an investor-led organization of governance professionals, in 2010 issued the ICGN Corporate Risk Oversight Guidelines to help institutional investors assess the effectiveness of a company's board overseeing risk management.[9] The guidelines rest on three key assumptions: (1) risk oversight begins with a company's board; (2) management is responsible for developing and executing strategic and operational risk management consistent with the strategy set by the board; and (3) shareholders have a responsibility to assess and monitor the risk oversight effectiveness of the board.[10] With regard to corporate risk oversight, the ICGN guidelines state that:

> The corporate board has a responsibility to take steps to assure that it has a proactive and dynamic approach that results in effective oversight of risk management. Strategy, risk tolerance, and risk are inseparable and should be connected in all discussions in the board… the board should hold the management accountable for developing a strategy that correlates with the risk tolerance of the organization. Boards are responsible for approving corporate strategy and risk tolerance.[11]

Financial Stability Board (FSB) The FSB was established to coordinate globally the development and implementation of regulatory and supervisory policies relating to the financial sector. Its members are national authorities responsible for financial stability, international standard-setting bodies, and central bank experts. On February 12, 2013, the FSB released a peer review report, *Thematic Review on Risk Governance*, based on a survey of its 24 member countries, that recommended that FSB member countries "should strengthen their regulatory and supervisory guidance…to assess the effectiveness of risk governance frameworks."[12] Specifically, the report recommended that boards be held accountable for oversight of the firm's risk governance and assess if the level and types of risk information provided to the board enable effective discharge of board responsibilities. The report stated that, "Boards should satisfy themselves that the information they receive from management and the control functions is comprehensive, accurate, complete, and timely to enable effective decision making on the firm's strategy, risk profile, and emerging risks.[13]

The report was followed in July by the release of a consultative document, *Principles for an Effective Risk Appetite Framework*, which stated 12 roles and responsibilities of the board with respect to the firm's risk appetite framework (RAF):[14]

1. approve the firm's RAF, developed in collaboration with the CEO, CRO [chief risk officer], and CFO, and ensure it remains consistent with the firm's short- and long-term strategy, business and capital plans, risk capacity, and compensation programs;
2. hold the CEO and other senior management accountable for the integrity of the RAF, including the timely identification, management, and escalation of breaches in risk limits and of material risk exposures;
3. ensure that annual business plans are in line with the approved risk appetite and incentives/disincentives are included in the compensation programs to facilitate adherence to risk appetite;
4. include an assessment of risk appetite in their strategic discussions including decisions regarding mergers, acquisitions, and growth in business lines or products;
5. regularly review and monitor actual versus approved risk limits (e.g., by business line, legal entity, product, risk category), including qualitative measures of conduct risk;
6. discuss and determine actions to be taken, if any, regarding "breaches" in risk limits;
7. question senior management regarding activities outside the board-approved risk appetite statement, if any;
8. obtain an independent assessment (through internal assessors, third parties, or both) of the design and effectiveness of the RAF and its alignment with supervisory expectations;
9. satisfy itself that there are mechanisms in place to ensure senior management can act in a timely manner to effectively manage, and where necessary mitigate, material adverse risk exposures, in particular those that are close to or exceed the approved risk appetite statement or risk limits;
10. discuss with supervisors decisions regarding the establishment and ongoing monitoring of risk appetite as well as any material changes in the elements of the RAF, current risk appetite levels, or regulatory expectations regarding risk appetite;
11. ensure adequate resources and expertise are dedicated to risk management as well as internal audit in order to provide independent assurances to the board and senior management that they are operating within the approved RAF, including the use of third parties to supplement existing resources where appropriate; and
12. ensure risk management is supported by adequate and robust IT and MIS [management information system] to enable identification, measurement, assessment, and reporting of risk in a timely and accurate manner.

UK Financial Reporting Council (FRC) On November 6, 2013, the FRC released a consultative draft proposing revisions to the UK Governance Code. According to this draft, the board's specific responsibilities in relation to risk include:[15]

- determining the extent to which the company is willing to take on risk (its "risk appetite");
- ensuring that an appropriate risk culture has been instilled throughout the organization;
- identifying and evaluating the principal risks to the company's business model and the achievement of its strategic objectives, including risks that could threaten its solvency or liquidity;
- agreeing how these risks should be controlled, managed, or mitigated;
- ensuring an appropriate risk management and internal control system is in place, including a reward system;
- reviewing the risk management and internal control systems and satisfying itself that they are functioning effectively and that corrective action is being taken where necessary; and
- taking responsibility for external communication on risk management and internal control.

The summary of board risk oversight developments noted here represents only a fraction of the global movement to hold boards more accountable for setting and overseeing management's risk appetite and risk tolerance and related supporting frameworks. Despite the rapid escalation of expectations, there has been little recognition that even the most expert, diligent, and well-meaning boards currently face major impediments to faithfully discharging these new fiduciary responsibilities.

Barriers to Effective Board Oversight of Risk

Asymmetric information: what boards don't know can hurt them Following the issuance of the 2009 Blue Ribbon Commission Report, the NACD, with the support of PwC and Gibson Dunn, in 2012 formed a new Advisory Council on Risk Oversight to identify and elevate leading risk oversight practices. The council has four goals:[16]

1. Discuss ways the board can get engaged in addressing risk areas.
2. Highlight the practices and processes the board should focus on.
3. Develop more precise definitions of risk oversight practices.
4. Identify the resources needed to effectively engage in those practices.

One challenge for boards identified during the council's deliberations was the risk of asymmetric information—the gap between the information known by management and the information presented to the board. The Advisory Council noted that:

> The role of a director, by nature, is a part-time job. As such, directors are reliant upon the executive team to provide information necessary to evaluate risks and corporate performance. Obviously, management cannot—and should not—provide every piece of data to the board. Thus, in selecting the information to be presented to directors, gaps can arise in what the C-suite is aware of as opposed to the board.
>
> Many believe these gaps have grown larger in recent years. "*The definition and role of oversight has changed in the last five years … [but] management hasn't realized that oversight has changed.*" Indeed, the expanding gaps may stem from management not fully realizing the new, changed board oversight role. While the board has to be comfortable with the reality of information asymmetry, directors should establish tolerance levels for the level of asymmetric risk they are willing to bear, and look for signs of when this risk has become too high.[17]

Difficulty determining "risk appetite" and "risk tolerance" Common language around risk is an essential starting point for effective enterprise-wide risk management.[18] Building a consensus around what "board oversight of management's risk appetite and tolerance" means in practice is an important step toward developing practical how-to strategies. Regulators, standard setters, and other influential organizations can assist by working together to provide clearer, widely agreed upon definitions of risk appetite and risk tolerance.

Unfortunately, at least to date, many boards have been reluctant to ask the CEO and senior management team direct and pointed questions designed to seek meaningful information that provides real insight into management's risk appetite and tolerance decision-making. Examples include:

- When making investments in complex financial instruments, what specific process is followed to determine your company's tolerance to these financial instruments, the soundness and safety of which were premised on the assumption that the US real estate market would continue to rise?
- How does the company determine its tolerance for violating laws and regulations?
- How does the company determine its tolerance for the risk that its employees may be violating the Foreign Corrupt Practices Act of 1977?

- How does the bank decide on tolerance levels to the risk that money laundering is occurring?
- What process is used to decide on the company's appetite linked to the risk that the company will need to restate its financial statements?
- Which line items in the financial statements and notes have the highest probability of being found to be materially misstated?
- How have we (management and the board) been deciding what is the "acceptable" level of employee injuries and fatalities?
- How does the company decide how many seriously dissatisfied customers are acceptable?
- How does the company decide on the acceptable level of risk linked to shipping defective, potentially dangerous products?
- Which business objectives key to our long-term success have retained risk positions that you consider (a) a little unacceptable? (b) somewhat unacceptable or (c) absolutely unacceptable?
- How much retained risk do we have right now in areas where compensation systems could cause generally good employees to commit illegal/unethical acts?

Most ERM frameworks provide limited or poor quality information on management's risk appetite/tolerance Boards must ensure that their organizations have effective risk management frameworks in place to allow them to oversee management's risk appetite and tolerance. Unfortunately, much of what is commonly referred to as enterprise risk management (ERM) has been implemented using a "risk-centric" approach where the focus is on risks without equal or greater focus ensuring clear linkage to related business objectives. Generally this approach involves conducting annual workshops and/or asking management via interviews and/or online surveys what they view as the firm's top risks. This annual update generates lists of the top 10, 20, or 50 risks along with an action plan to address "red rated" risks, risks where the current mitigation efforts are considered inadequate. The lists are periodically presented to the board, usually annually. Risk "heat maps" and risk "traffic lights" are frequently used as key communication vehicles.

Unfortunately, our observation is that only a minority of risk management frameworks in use today require formal risk assessments of the organization's top strategic business objectives, and they often lack a formal process to identify business objectives that have been statistically shown to have a high likelihood of significantly eroding shareholder value. Although there is an urgent need for more research in this area, this observation is generally supported by survey results that indicate that current linkages between strategic planning, compensation systems, and formal risk assessment processes are still low globally.[19] The linkage between the risks periodically reported to the boards and the objectives that are most critical to the long-term success of the company is at best often opaque, and at worst, missing completely.

The risk-centric approach in use by most organizations identifies and evaluates risks in isolation. In reality, most important end-result business objectives are impacted by 10 or more significant risks that often are interrelated (for example, objectives to ensure compliance with laws in all jurisdictions in which the company operates and to increase market share by 10 percent year over year). Such risk-centric approaches often do not formally enumerate the full range of treatments in place for the identified risks. When attempts are made to identify linked risk treatments, the focus is often on documenting only what are generally broadly known as "internal controls." Boards are rarely told about viable risk treatments used effectively by other companies to reduce retained/residual risk levels that management has consciously, or unconsciously, elected not to employ.[20] The methods not selected to treat/mitigate key risks are often as relevant to decision makers as the methods that were chosen. Risk transfer, risk financing, risk sharing, risk avoidance, and risk acceptance vehicles, even when key to the real corporate risk treatment strategy, often are not formally considered or included in the risk information presented to boards.

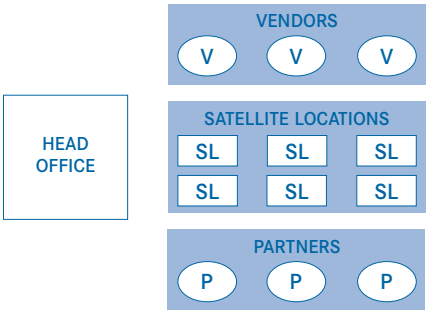
Traditional internal audit approaches do not provide information for decisions on entity-wide residual/ retained risk status Traditional "direct report" approaches to internal audit (where internal auditors function as the primary formal risk/control analysts/reporters to the board) call for the chief internal audit executive to use what is often loosely referred to as a "risk-based" audit approach. In our experience, when performing their risk assessments, internal auditors rarely utilize the risk assessment methods advocated by global risk standards like ISO 31000. Decisions are often made based on some arbitrary risk factors linked to topics, business areas, or issues to be included in the upcoming audit cycle for conducting point-in-time audits, such as time since last audit, number of audit findings in the last audit, size of assets, maturity of management, and other factors that haven't been empirically validated as true risk predictors. Then, based on budget or management priority, a percentage of the audits chosen are completed and results are reported to senior management, and in some cases, the audit committee. These point-in-time assessments usually represent only a small percentage of an organization's total risk universe.

Figure 1 provides more details on what we often reference as the "historical approach" to internal audits. In addition to serious coverage limitations and auditor subjectivity about what constitutes "effective" control, the level of rigor used to assess the areas selected by internal audit varies enormously from firm to firm. Boards often are not informed about which areas/topics were rigorously assessed, which received only cursory attention, and which have never been audited at all.

Figure 1

Historical audit approach to direct reporting on control "adequacy" or "effectiveness"

AUDIT UNIVERSE



Characteristics of this approach:

1 Auditors examine and report on the adequacy" or "effectiveness" of controls related to specified topics or business cycles. Audits are often done on a cyclical basis and opinions issued at the end of each assignment. Alternatively, a "risk-based" approach developed by an audit group may be used in place of, or in addition to, a cyclical plan.

2 Audit cycles generally range from annual to infinity (i.e., some topics/areas/locations are never audited).

3 Auditors usually maintain some type of audit universe or audit planning framework that provides the logic and/or justification for the areas audited. One example of a risk formula developed by internal audit uses 19 variables. Ratings are assigned by internal audit judgmentally based on available knowledge and information.

4 Cyclical audit approaches are generally premised on relatively low rates of change in the business environment. Although high rates of change theoretically require increased frequency of audit coverage, audit resource constraints often preclude reacting to this information.

5 If high reliability is required by clients on the reports provided by the internal auditors, the amount of work required is substantial. (Note: It is likely that if internal auditors had personal legal liability for opinions expressed on control effectiveness, as is the case for external auditors reporting on financial statements, internal audit coverage and approach strategy would change in virtually all organizations).

6 Audit departments sometimes maintain or increase audit frequency by reducing topics covered and/or the depth of coverage. This often impacts on reliability levels that can be attached to the audit findings and opinions expressed. Opinions from internal auditors are rarely accompanied by information on the reliability of the opinion.

7 Auditors are often measured primarily on whether they complete their audit plan on a timely basis and whether customers are happy.

8 Examples of audit topics covered using this method include:

- payables
- receivables
- product inventory
- cash
- derivatives
- materials and supplies
- safety
- environment
- systems access controls

Alternatively, these audits may be arranged on a cycle or process basis. Examples include:

- sales/revenue cycle
- disbursements/pay cycle
- production cycle
- account consolidation process
- environmental incident management
- claims payment process

9 Audit usually functions as the primary control analyst/reporter in this approach. Clients usually assume that, where a topic is included within the disclosed audit scope and the auditor raises no issues, the controls must be "adequate" and/or "effective."

10 When auditors do report one or more control deficiencies or areas for improvement, it implies that they have concluded that the related risks are, or may be, unacceptable and outside of the organization's risk appetite/tolerance.

11 Auditors rarely report explicitly to the board the business objectives or topics not covered, or the major risks deemed to be acceptable by management and internal audit. Reports typically focus only on what they elected to review with the resources available.

Examples of variables used in a risk formula developed by internal audit:

- quality of internal control
- competence of management
- integrity of management
- size of unit ($)
- recent change in accounting system
- complexity of operations
- liquidity of assets
- recent change in key personnel
- economic condition of unit
- rapid growth
- extent of computerized systems
- time since last audit
- pressure on management to meet objectives
- extent of government relations
- level of employees' morale
- audit plans of external auditors
- political exposure
- need to maintain an appearance of independence by internal auditor
- distance from main office

In most organizations, internal auditors still focus on reporting subjective opinions on the effectiveness controls, absent any clear indication of the level and types of retained/residual risks that are acceptable to senior management and the board. These historical audit approaches are often a combination of testing for compliance with policies, testing "key internal controls," evaluating business processes, and/or assessing whether the organization conforms to the criteria of a particular control framework, most often the 1992 legacy Committee of Sponsoring Organizations (COSO) control framework. Unfortunately, these audit methods do not provide the breadth and depth of information necessary for boards to effectively oversee management's risk appetite and tolerance. The 2008 global financial crisis is a case in point—based on publicly available information, few, if any, internal audit departments of the suspect companies alerted their boards to the massive retained risk levels being accepted by management.[21] Similarly, a large percentage of these organizations were deemed by their CEOs, CFOs, and external auditors to have effective internal controls in accordance with the 1992 COSO internal control framework.

Lack of agreement on "effective" risk governance Credit rating agencies, smarting from a barrage of criticism of their track record leading up to the 2008 global financial crisis, continue to grapple with how to include risk governance elements in their credit rating reviews. In a 2009 progress report, Standard & Poor's reported lack of "clear examples of definitions for risk tolerance or risk appetite"[22] as a key obstacle to adequately assessing credit risk exposures.

There is still little information made available to the capital markets that informs stakeholders about how credit rating agencies incorporate the effectiveness of a company's risk management practices and processes into their models. The reason for the lack of clarity is simple—credit rating agencies themselves are still struggling to reach some general agreement on what an effective risk management framework should look like. Boards are similarly challenged with respect to the questions they should be asking in this area and the business processes they should be actively overseeing to discharge their onerous new fiduciary duties relating to risk oversight.

Litigation risk Truly effective risk management provides transparency and disclosure about deliberate business decisions to accept risk. However, that can be a double-edged sword for boards.

In litigious societies, particularly the United States, knowledge of a risk acceptance decision by senior management and sometimes the board, in the possession of a regulator, criminal prosecutor, or plaintiffs' bar armed with the benefit of hindsight, can significantly increase personal and corporate legal exposure for board members if the decision to accept such risk turns out badly for shareholders, key stakeholders, or society generally. This litigation risk must be carefully weighed against the possibility that not formally assessing and managing risks can be viewed by regulators and the courts as negligent, or even a breach of management's and the board's fiduciary duty of care.

The good news for boards is that the Delaware Chancery Court so far has been reluctant to hold directors personally liable for inadequate or failed risk management, as evidenced by the court's decision in the Citigroup Inc. shareholder derivative litigation:

> The Delaware Chancery Court's reluctance to impose liability on Citigroup's directors for allegedly failed or inadequate risk management practices is consistent with the general notion that business decisions should be made in the boardroom and not the courtroom. It also reflects the complexity of assessing business risk and the delicate balance between risk and return. As Chancellor Chandler stated, "Business decision-makers must operate in the real world, with imperfect information, limited resources, and an uncertain future. To impose liability on directors for making a 'wrong' business decision would cripple their ability to earn returns for investors by taking business risks."[23]

Boards don't ask for the information they need Lastly, arguably the biggest single handicap that boards of directors face today in doing a better job overseeing management's risk appetite and risk tolerance is self-inflicted. Many boards, for a variety of reasons, including the rationale that "this is how we've always done it" or "it would be impolite to ask," have simply not asked senior management and other relevant parties for the type, quality, and quantity of information necessary to meet increased risk oversight and risk governance expectations. Directors must ask themselves, "Who has real control of the agenda for board meetings? Are we as a board meaningfully influencing the type and quantity of retained risk status information provided by management, internal auditors, risk functions, chief legal counsel, external auditors, and other key players?"

A Board-Driven Approach, or Objective-Centric Risk Governance

In this section, we offer eight recommendations for boards that want to meet the new risk oversight expectations.

1 **Transform the risk management and assurance functions from "supply driven" to "board/demand driven."** For a variety of reasons, boards have not devoted much time or consideration to detailing specifically what they want from internal and external auditors or from the ERM function, if one exists. These assurance providers have, for the most part, been "supply driven," largely making their own decisions about what information is supplied to boards of directors and senior management to help them discharge their fiduciary responsibilities. The emergence of globally codified board risk oversight expectations requires that boards demand better quality information about risk management and risk oversight processes, and formal written opinions on their effectiveness from assurance providers.

2 **Clarify accountability.** Boards should actively discuss the new board risk oversight expectations, decide which expectations are most relevant to the organization, and agree on a corporate strategy to meet them. To start, directors should agree upon and document the core end results expected from each participant in the risk governance process. Exhibit 1 (p. 10) provides a sample board-driven, objective-centric risk management policy, including suggested accountabilities for the board, CEOs, senior management, work units, and specialist assurance groups.

3 **Focus on end-result objectives.** ISO 31000, the most globally accepted risk management standard, defines risk as the "effect of uncertainty on objectives."[24] Unfortunately, it's our experience that a large portion of the risk and control work done today lacks a visible link between risks and end-result objectives, and often fails to focus resources on assessing the risks to the objectives that are most important to value creation or that have the highest probability of eroding entity value. All risk assessment work overseen by the board and completed by the senior management, internal audit, external audit, safety, environment, quality, compliance, and work units should employ an objective-centric risk assessment process that actively supports the straightforward ISO 31000 risk definition.[25] Exhibit 2 (p. 12) provides an example of an objective-centric risk assessment approach that creates a composite snapshot of the current "residual risk status" linked to the specific objective or objectives being assessed, including information on current performance levels and the impact of nonachievement of the objective in whole or part. This approach, unlike traditional risk-centric ERM methods that assess the range of likelihood and impact of a single risk and risks in isolation, is designed to assist management and boards in determining whether the current retained risk position linked to key value creation and potentially value eroding objectives is within collective corporate risk appetite and tolerance. It explicitly links risks, risk treatments, and performance information, and encourages identification and disclosure of viable risk treatments not selected by the management.

   The decision on the acceptability of the current retained/residual risk status can be followed by steps to assess whether the current risk treatment strategy is "optimized," meaning that the current risk treatment design is the lowest cost risk treatment strategy capable of producing an acceptable level of retained risk. Our observation is that few boards receive much, if any, information from internal audit or ERM support functions on whether risk treatments are optimized.

4 **Change internal audit's mandate and reporting.** In many organizations, internal audit's primary mandate is to plan, complete, and report the results of spot-in-time audits to work units, senior management, and the board. In many cases internal auditors form subjective opinions on whether they believe "controls" are effective without truly knowing the risk appetite and tolerance of senior management and the board. Management is often under significant pressure to remediate any identified unmitigated risks, regardless of whether there are other areas that represent far greater opportunities or threats to the long-term success of the entity. A strong argument can be made that traditional direct report internal audit (where internal audit functions as the primary risk/control analyst and reporter) often results in suboptimal and distorted misallocation of corporate resources, which can be amplified by well-meaning boards that believe it is part of their job to ensure that internal audit findings and recommendations are addressed by management.[26]

   A more useful mandate is for the internal audit function to assess and report on the effectiveness of an organization's risk management processes (or "Risk Appetite Framework"[27]) and the reliability of the consolidated reports on the organization's overall risk profile and state of residual/retained risk provided by the CEO or other member of the senior management team to the board. Reporting on the effectiveness of risk management processes is being cautiously championed by the Institute of Internal Auditors (IIA) globally through its International Professional Practice Framework (IPPF) Standard #2120, and through the creation of a new professional certification, Certification in Risk Management Assurance (CRMA).[28]

5 **Change the mandate of ERM functions.** Regulators have demanded the implementation of formal ERM frameworks in many organizations, particularly financial services firms. As previously discussed, calls for demonstrable board risk oversight are expected to increase significantly in the years ahead. Unfortunately many ERM projects degenerate into an annual compliance exercise of updating risk registers to present the top 10 (or 50) risks to the board, rather than providing meaningful and actionable retained risk status information for boards.

   ERM functions should be tasked with assisting with the implementation and maintenance of risk appetite frameworks capable of meeting the type of risk oversight expectations espoused by the NACD, the FSB, and the FRC.

6 **Demand information on risks posed by reward systems.** Compensation/reward systems, which were identified by the SSG as one of the areas of weakness that required further work by financial firms, not only played a key role in the global crisis but also significantly influenced the other root causes. The SEC, as part of new proxy disclosure risk oversight reporting requirements adopted in 2009, requires US public companies to disclose the steps their boards have taken to identify misaligned, high-risk reward systems.

   Boards should explicitly demand information on a regular basis from assurance providers and senior management teams about the potential risks to the company posed by misaligned reward systems.

7 **Recognize the need for training.** A large percentage of boards are composed of senior business executives with decades of experience confronting and managing all kinds of risks on a daily basis. Not surprisingly, most board efforts to oversee management's risk appetite and tolerance have been similarly intuitive and lacking in formality and transparency. However, a "gut feel" approach to risk management is untenable if the goal is to meet escalating board risk governance expectations.

   Boards should ensure a formal assessment process is in place to identify risk governance skill and knowledge gaps for all key players in the company, including the board, and a clear-cut plan to close any gaps. Boards can lead by example by requesting an entity-level risk management and governance skill and knowledge gap assessment and a training plan to remediate any deficiencies. This will send a strong signal to other key risk governance players, including senior management and work units, that the status quo is no longer sufficient.

8 **Recognize and accept that better-documented risk management is a "two-edged sword."** As boards and companies implement more transparent and demonstrable risk management systems, somewhat ironically, they will almost certainly elevate their levels of litigation and regulatory risk. Better and more formal risk management processes have the potential to "burden" boards with documented knowledge of risk acceptance and risk tolerance decisions that have the potential to implode. This risk must be fully understood and risk strategies must be put in place to address it.

Conclusion

Expectations for board oversight of risk are rapidly evolving, and most boards will face significant challenges in meeting those new expectations. Many current approaches to risk oversight often fail to link risks to strategic business objectives. We recommend that boards take action to implement a board-driven approach that links retained risk information to strategic and foundation business objectives and increase the certainty of achieving them.

Exhibit 1

Sample Board–Driven, Objective-Centric Corporate Risk Management Policy

Purpose:

The purpose of this policy is to create, enhance and protect shareholder value by designing, implementing and maintaining an effective, structured, and enterprise-wide risk management approach. We believe that adopting this policy will result in both immediate and long-term benefits to internal and external stakeholders, such as:

- Increasing the likelihood of achieving the company's business objectives
- Enhancing XYZ's competitive advantage
- Dealing more effectively with market instability
- Enabling XYZ to better meet customer expectations and contractual requirements
- Establishing a board-level mandate to implement an enterprise-wide approach to risk management to meet emerging risk management and risk oversight expectations from regulators and standard setters
- Enhancing shareholder and customer confidence
- Responding to institutional shareholder demands for effective risk management frameworks in the companies in which they invest
- Meeting credit rating agency expectations related to risk management

Scope

This policy applies to employees, officers and directors of XYZ Corp. and its subsidiaries. References in this policy to the Corporation mean XYZ Corp. and its subsidiaries.

Policy

1.1 Risk Management Principles

Risk management is a systematic, structured, transparent, inclusive, and timely way to manage uncertainty and create and protect shareholder value. It should be adaptive to XYZ's business needs and a dynamic process. It should evaluate risk/reward trade-offs within the corporation's risk appetite and tolerance.

It is intended to be an integral part of all organizational processes, including strategic planning and decision making, and is based on best available, "fit for purpose" risk information. It is dynamic, iterative, and facilitates continuous improvement of the organization.

2.1 Corporate Risk Assessment Methodology

The risk assessment methodology the corporation has selected focuses on end-result business objectives that the company must achieve to be successful and drive sustained shareholder value. The key goal is identification and consensus agreement on the acceptability of the company's retained risk position (retained risk position is a composite snapshot that helps decision makers and the board better understand the level of uncertainty that exists that business objectives will not be achieved).The risk management methods and tools used by the corporation are expected to evolve and mature over time with an overriding goal that the amount of formal risk assessment applied (as opposed to informal risk management which happens every day in every part of the corporation) will be determined by carefully considering the costs and benefits of the additional information.

3.1 Risk Management Roles and Responsibilities

The **Board of Directors** is responsible for:

a. approving and authorizing this policy
b. assessing whether the risk appetite and tolerance implicit in the corporation's business model, strategy, and execution is appropriate
c. assessing whether the expected risks in the corporation's strategic plan are commensurate with the expected rewards
d. evaluating whether management has implemented an effective and fit-for-purpose process to manage, monitor, and mitigate risk that is appropriate given the corporation's size, growth aspirations, business model, and strategy
e. assessing whether the corporation's risk management processes are capable of providing reliable information to the board on the major risks facing the corporation, including significant risks to the corporation's reputation and key value creation and potentially value eroding objectives

The **CEO** is responsible for:

a. appointing the members of the corporation's risk oversight committee
b. assessing whether the corporation's current and expected risk status is appropriate given the corporation's and board of directors' risk appetite and tolerance
c. ensuring reliable processes are in place to provide the board of directors with an annual report on the effectiveness of the corporation's risk management procedures, and periodic reports on the corporation's consolidated residual risk status, including remediation actions underway to adjust the corporation's retained risk position

The **Risk Oversight Committee** is responsible for:

a. determining where and when formal documented risk assessments should be completed, recognizing that additional risk management rigor and formality should be cost/benefit justified

b. ensuring that business units are identifying and reliably reporting the material risks to the key objectives identified in their annual strategic plans and core foundation objectives necessary for sustained success, including compliance with applicable laws and regulations

c. reviewing and assessing whether material risks being accepted across XYZ are consistent with the corporation's risk appetite and tolerance

d. developing, implementing, and monitoring overall compliance with this policy

e. overseeing development, administration and periodic review of this policy for approval by the board of directors

f. reviewing and approving the annual external disclosures related to risk oversight processes required by securities regulators

g. reporting periodically to the CEO and the board on the corporation's consolidated residual risk position

h. ensuring that an appropriate culture of risk-awareness exists throughout the organization

Business unit leaders are responsible for:

a. managing risks to their unit's business objectives within the corporation's risk appetite/tolerance

b. identifying in their business unit's annual strategic plan the most significant internal and external risks that have the potential to impact on the business unit's key objectives, as well as the risk treatment vehicles and plans to address those risks

c. reporting to the risk management support services unit the current composite residual risk rating ("CRRR") on key objectives identified in the business unit's strategic plan and other objectives that may have been assigned to them by the risk oversight committee and/or the CEO

d. completing documented risk assessments when they believe the benefits of formal risk assessment exceed the costs, or when requested to by the CEO or risk oversight committee

Risk management and assurance support services unit is responsible for:

a. providing risk assessment training, facilitation, and assessment services to senior management and business units upon request

b. annually preparing a consolidated report on XYZ's most significant residual risks and related residual risk status, and a report on the current effectiveness and maturity of the Corporation's risk management processes for review by the risk oversight committee, senior management, and the corporation's board of directors

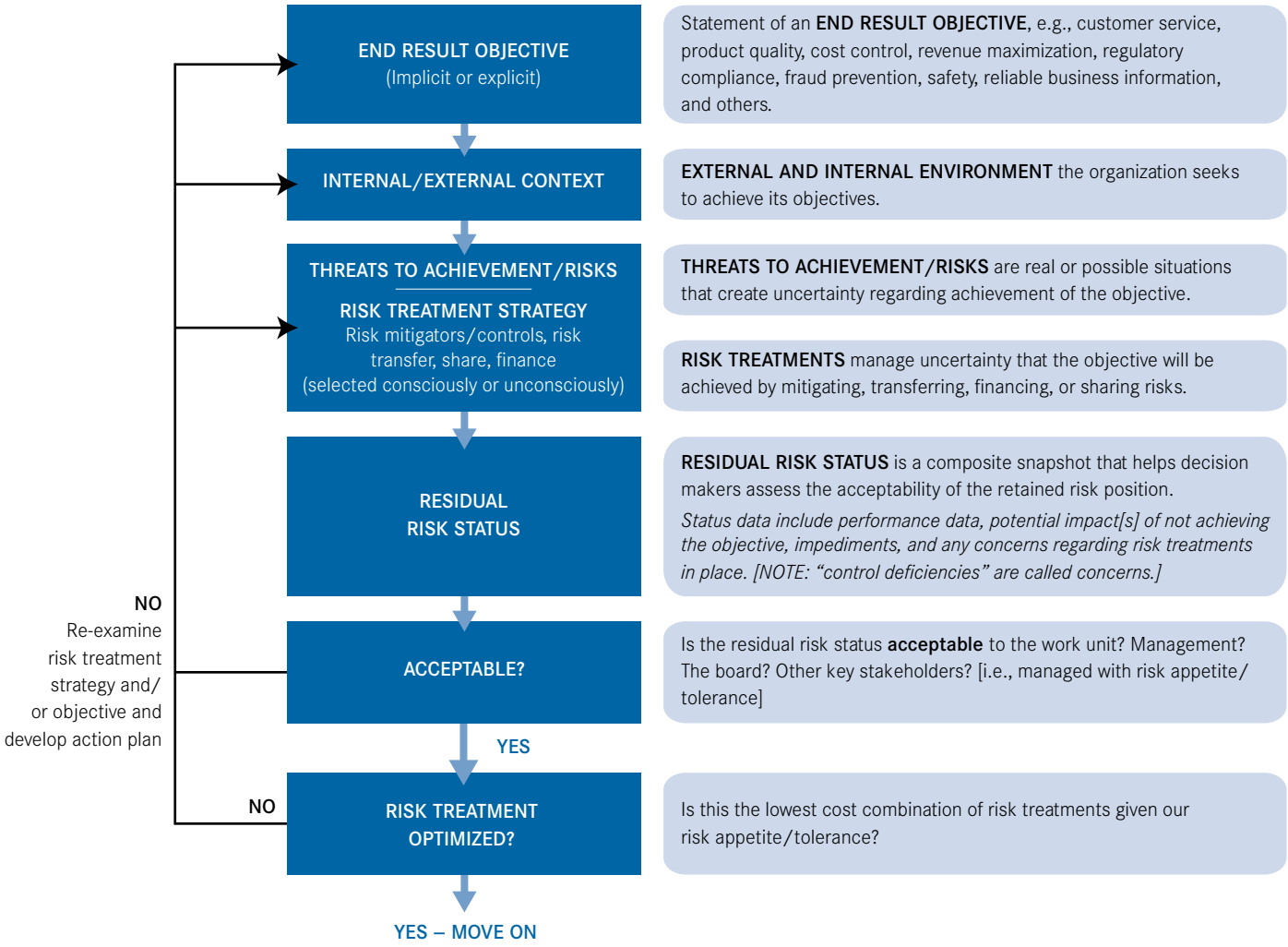
c. completing risk assessments of specific objectives that have not been formally assessed and reported on by business units when asked to by the risk oversight committee, senior management, or the board of directors; or if the risk management support services team leader believes that a formal risk assessment is warranted to provide a materially reliable risk status report to senior management and the board of directors

d. conducting independent quality assurance reviews on risk assessments completed by business units and providing feedback to enhance the quality and reliability of those assessments

e. participating in the drafting and review of the corporation's annual disclosures in the Annual Reports and Proxy Statement related to risk management and oversight

Exhibit 2

Objective-centric risk assessment approach



Source: Risk Oversight, Inc., 2012.

Endnotes

1 For the purposes of this report, we assume that board oversight of management's risk appetite and tolerance requires, by extension, that the board also oversee the effectiveness of the processes that produce the information used to discharge that responsibility (i.e., an entity's entire risk management framework).

2 See *Observations on Risk Management Practices during the Recent Market Turbulence*, Senior Supervisors Group, March 6, 2008 (last accessed on September 5, 2013 at www.newyorkfed.org/newsevents/news/banking/2008/SSG_Risk_Mgt_doc_final.pdf), and Risk Management Lessons from the Global Banking Crisis of 2008, Senior Supervisors Group, October 21, 2009 (last accessed on September 5, 2013 at www.sec.gov/news/press/2009/report102109.pdf).

3 The term "risk appetite and tolerance" is evolving. See "Principles for an Effective Risk Appetite Framework," the Financial Stability Board, July 17, 2013, p. 2 (www.financialstabilityboard.org/publications/r_130717.pdf) which defines "risk appetite" as, "The aggregate level and types of risk a firm is willing to assume within its risk capacity to achieve its strategic objectives and business plan." The term "risk capacity" is often used as a synonym for "risk tolerance."

4 "Risk Governance: Balancing Risks and Rewards," National Association of Corporate Directors Blue Ribbon Commission, October 2009, p. 4 (www.nacdonline.org/Store/ProductDetail.cfm?ItemNumber=675).

5 Matteo Tonello, *The Role of the Board in Turbulent Times: Leading the Public Company to Full Recovery*, The Conference Board, Research Report 1452, September 2009, p. 13.

6 U.S. Securities and Exchange Commission, "Final Rule on Proxy Disclosure Enhancements," Release Nos. 33-9089 and 34-61175, effective February 28, 2010, p. 44 (www.sec.gov/rules/final/2009/33-9089.pdf). Last accessed September 5, 2013.

7 Public Statement by SEC Commissioner Luis A. Aguilar, "Shareholders Need Robust Disclosures to Exercise Their Voting Rights as Investors and Owners," February 20, 2013 (www.sec.gov/News/PublicStmt/Detail/PublicStmt/1365171492322). Last accessed on September 5, 2013.

8 Section 165(h) of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (www.gpo.gov/fdsys/pkg/BILLS-111hr4173enr/pdf/BILLS-111hr4173enr.pdf). Last accessed on September 6, 2013.

9 International Corporate Governance Network, "ICGN Corporate Risk Oversight Guidelines," October 2010, available at www.accaglobal.com/content/dam/acca/global/PFD-memberscpd/AFF/ICGN-oversight-guidelines.pdf.

10 ICGN Corporate Risk Oversight Guidelines, p. 5.

11 ICGN Corporate Risk Oversight Guidelines, p. 8.

12 *Thematic Review on Risk Governance*, Financial Stability Board, February 12, 2013, p. 4 (www.financialstabilityboard.org/publications/r_130212.htm). Last accessed on September 5, 2013

13 *Thematic Review on Risk Governance*, p. 4.

14 "Principles for an Effective Risk Appetite Framework Consultative Document," Financial Stability Board, July 17, 2013, p. 7.

15 "Risk Management, Internal Control and the Going Concern Basis of Accounting: Consultation on Draft Guidance to the Directors of Companies Applying the UK Corporate Governance Code and Associated Changes to the Code," Financial Reporting Council, November 2013, p. 24 (www.frc.org.uk/Our-Work/Publications/FRC-Board/Consultation-Paper-Risk-Management,-Internal-Contr-File.pdf).

16 "Advisory Council on Risk Oversight: Summary of Proceedings," National Association of Corporate Directors, May 1, 2013, p. 2. (http://nacd.files.cms-plus.com/AC%20on%20Risk%20Oversight%20Summary_Final.pdf). Last accessed on September 6, 2013.

17 "Advisory Council on Risk Oversight: Summary of Proceedings," p. 5. (emphasis in original).

18 James W. DeLoach, *Enterprise-wide Risk Management: Strategies for Linking Risk and Opportunity* (London: Prentice-Hall/Financial Times, 2000).

19 For example, see "2013 Global Risk Management Survey," Aon Risk Management Solutions (www.aon.com/2013GlobalRisk/default.jsp); Carolyn Kay Brancato et al., *The Role of US Corporate Boards in Enterprise Risk Management*, The Conference Board, Research Report 1390-06, July 2006; Mark S. Beasley, Bruce C. Branson, and Bonnie V. Hancock, *COSO's 2010 Report on Enterprise Risk Management*, December 2010; "Global Survey on Risk Management and Internal Control," International Federation of Accountants Professional Accountants in Business Committee, February 2011; Andre Brodeur, Kevin Buehler, Michael Patsalos-Fox, and Martin Pergler, "A Board Perspective on Enterprise Risk Management," McKinsey & Company, February 2010; "Report on the Accenture 2011 Global Risk Management Survey," Accenture, June 29, 2011; "Corporate Governance: Building Better Boards," Thomson Reuters (http://accelus.thomsonreuters.com/sites/default/files/Corporate-Governance-Building-Better-Boards.pdf); Carlo Corsi, Julie Hembrock Daum, Willi Schoppen, and Justin Menkes, "Five Things Directors Should Be Thinking About," SpencerStuart, December 2010; and *Thematic Review on Risk Governance*, FSB.

20 On the risk-centric approach to ERM, see Tim Leech, "The High Cost of 'ERM Herd Mentality,'" Risk Oversight, March 2012 (http://riskoversight.ca/wp-content/uploads/2011/03/Risk_Oversight-The_High_Cost_of_ERM_Herd_Mentality_March_2012_Final.pdf). Last accessed on September 6, 2013.

21 Under the current IIA 2120 guidance some internal audit departments may be able to claim that they assessed management's risk processes by doing traditional point-in-time internal audits; however, the point is not just to comply with the standard but also to assure the boards that the residual risk status of the company is within the risk appetite and tolerance they set.

22 "Progress Report: Integrating Enterprise Risk Management Analysis into Corporate Credit Ratings," Standard & Poor's, July 22, 2009 (http://www.standardandpoors.com/ratings/erm/en/us).

23 Michelle Harner, "Barriers to Effective Risk Management," *Seton Hall Law Review*, 2011, p.22 (http://erepository.law.shu.edu/cgi/viewcontent.cgi?article=1070&context=shlr). Last accessed on September 6, 2013.

24 I*SO 31000:2009, Risk Management—Principles and Guidelines*, International Organization for Standardization, 2009, p. 1.

25 For more on the "objective-centric" approach, see, "A Global Perspective on Assessing Internal Control Over Financial Reporting," Institute of Management Accountants, September 2006 (www.leechgrc.com/pdf/kb-sps/A%20Global%20Perspective%20on%20Assessing%20IC.pdf). Last accessed on September 6, 2013.

26 Leech, "The High Cost of 'ERM Herd Mentality.'"

27 See "Principles for an Effective Risk Appetite Framework."

28 See Standards and Guidance—International Professional Practices Framework (IPPF)® (https://na.theiia.org/standards-guidance/Pages/Standards-and-Guidance-IPPF.aspx) and Certification in Risk Management Assurance™ (CRMA®) (https://na.theiia.org/certification/crma-certification/Pages/CRMA-Certification.aspx).

About the Authors

Parveen P. Gupta is the chair and professor of accounting at the College of Business and Economics at Lehigh University in Bethlehem, Pennsylvania. He is a recognized expert in Sarbanes-Oxley, internal control, risk management, financial reporting quality, and corporate governance. He has published numerous research papers and monographs in these areas. He is the recipient of many awards in teaching and research. During 2006–2007, he served as an academic accounting fellow in the SEC Division of Corporation Finance, where he worked closely with the division's chief accountant and participated actively on Sarbanes-Oxley–related projects involving issuing Commission's Guidance on Management's Report on Internal Control under Sarbanes-Oxley Act Section 404 and Public Company Accounting Standard Board's (PCAOB) Auditing Standard No. 5 on Auditing Internal Control. He and his team members were recognized for their work in this area with the "Law and Policy" award. His advisory experience is in the related areas and includes working with US-based manufacturing, financial services, energy industry clients and Big Four public accounting firms. He is a frequent speaker at academic and professional conferences both at a national and international level. He is often quoted in the media.

Tim J. Leech is managing director, global services at Risk Oversight Inc. based in Oakville, Ontario. He is recognized globally as a thought leader, innovator, and provocateur in the risk and assurance fields. He has provided ERM training and consulting services and technology to public and private sector organizations in Canada, the United States, the United Kingdom, Europe, Australia, South America, Africa, the Middle East, and Asia. Tim and his daughter Lauren coauthored a 2011 paper published in the International Journal of Disclosure and Governance titled, "Preventing the Next Wave of Unreliable Financial Reporting: Why Congress Should Amend Section 404 of the Sarbanes-Oxley Act." For The Conference Board, he authored, "Board Oversight of Management's Risk Appetite and Tolerance." He lives in Oakville, Ontario, with Elaine, his wife for over 38 eventful years.

Acknowledgments

The authors would like to thank the following individuals for reviewing and providing feedback on earlier versions of this report: James K. Wright, general auditor, Tep Inc.; Grant Purdy, associate director, Broadleaf Capital International Pty Ltd; Norman Marks, OCEG fellow and honorary fellow of the Institute of Risk Management; Paul Sobel, vice president and chief audit executive, Georgia-Pacific LLC; Vincent Tophoff, International Federation of Accountants; John Fraser, HydroOne; and Lauren Leech.

About Director Notes

Director Notes is a series of online publications in which The Conference Board engages experts from several disciplines of business leadership, including corporate governance, risk oversight, and sustainability, in an open dialogue about topical issues of concern to member companies. The opinions expressed in this report are those of the author(s) only and do not necessarily reflect the views of The Conference Board. The Conference Board makes no representation as to the accuracy and completeness of the content. This report is not intended to provide legal advice with respect to any particular situation, and no legal or business decision should be based solely on its content.

About the Series Director

Matteo Tonello is managing director of corporate leadership at The Conference Board in New York. In his role, Tonello advises members of The Conference Board on issues of corporate governance, regulatory compliance, and risk management. He regularly participates as a speaker and moderator in educational programs on governance best practices and conducts analyses and research in collaboration with leading corporations, institutional investors, and professional firms. He is the author of several publications, including *Corporate Governance Handbook: Legal Standards and Board Practices*, the annual *US Directors' Compensation and Board Practices* and *Institutional Investment* reports, and *Sustainability in the Boardroom*. Recently, he served as the co-chair of The Conference Board Expert Committee on Shareholder Activism and on the Technical Advisory Board to The Conference Board Task Force on Executive Compensation. He is a member of the Network for Sustainable Financial Markets. Prior to joining The Conference Board, he practiced corporate law at Davis, Polk & Wardwell. Tonello is a graduate of Harvard Law School and the University of Bologna.

About the Executive Editor

Melissa Aguilar is a researcher in the corporate leadership department at The Conference Board in New York. Her research focuses on corporate governance and risk issues, including succession planning, enterprise risk management, and shareholder activism. Aguilar serves as executive editor of *Director Notes*, a bimonthly online publication published by The Conference Board for corporate board members and business executives that covers issues such as governance, risk, and sustainability. She is also the author of The Conference Board *Proxy Voting Fact Sheet* and coauthor of *CEO Succession Practices*. Prior to joining The Conference Board, she reported on compliance and corporate governance issues as a contributor to *Compliance Week* and *Bloomberg Brief Financial Regulation*. Aguilar previously held a number of editorial positions at SourceMedia Inc.

About The Conference Board

The Conference Board is a global, independent business membership and research association working in the public interest. Our mission is unique: to provide the world's leading organizations with the practical knowledge they need to improve their performance and better serve society. The Conference Board is a nonadvocacy, not-for-profit entity, holding 501(c) (3) tax-exempt status in the USA.

About The Conference Board Governance Center®

The Conference Board Governance Center brings together a distinguished group of senior corporate executives from leading world-class companies and influential institutional investors in a collaborative setting. As a member of the Governance Center, you will participate in a thought-leading forum to engage with other corporate executives and institutional investors in a confidential, collaborative setting; hear from outside experts about emerging issues; discuss and get counsel on your most pressing governance, ethics, and enterprise risk challenges; examine issues from an interdisciplinary perspective; and drive landmark research that contributes to advancing best practices. For more information, please visit www.conference-board.org/governance.

For more information on this report, please contact:
Melissa Aguilar, researcher, corporate leadership at 212 339 0303 or melissa.aguilar@conferenceboard.org

THE CONFERENCE BOARD, INC. | WWW.CONFERENCEBOARD.ORG
AMERICAS | +1 212 759 0900 | CUSTOMER.SERVICE@CONFERENCEBOARD.ORG
ASIA | +65 6325 3121 | SERVICE.AP@CONFERENCEBOARD.ORG
EUROPE, MIDDLE EAST, AFRICA | +32 2 675 54 05 | BRUSSELS@CONFERENCEBOARD.ORG

THE CONFERENCE BOARD OF CANADA | +1 613 526 3280 | WWW.CONFERENCEBOARD.CA

To learn more about The Conference Board corporate membership, please email us at membership@conferenceboard.org