Director Notes

The Next Frontier for Boards: Oversight of Risk Culture

by Parveen P. Gupta and Tim Leech

Over the past 15 years expectations for board oversight have skyrocketed. In 2002 the Sarbanes-Oxley Act put the spotlight on board oversight of financial reporting. The 2008 global financial crisis focused regulatory attention on the need to improve board oversight of management's risk appetite and tolerance. Most recently, in the wake of a number of high-profile personal data breaches, questions are being asked about board oversight of cyber-security, the newest risk threatening companies' long term success.[1] This article provides a primer on the next frontier for boards: oversight of "risk culture."

Weak "risk culture" has been diagnosed as the root cause of many large and, in the words of the Securities and Exchange Commission Chair Mary Jo White, "egregious" corporate governance failures.[2] Deficient risk and control management processes, IT security, and unreliable financial reporting are increasingly seen as mere symptoms of a "bad" or "deficient" risk culture. The new challenge that corporate directors face is how to diagnose and oversee the company's risk culture and what actions to take if it is found to be deficient.

Regulators, institutional investors, and credit rating agencies have increased the call for corporate directors to strengthen board governance and board risk oversight. The Enron era saw boards of directors being accused of fiduciary failure for allowing "high risk accounting."[3] Sarbanes-Oxley raised the bar significantly in the area of financial reporting for audit committees, CEOs, and CFOs of US listed public companies. In the aftermath of the global financial crisis of 2008, regulators have reached a consensus: boards should be evaluated and put on the regulatory hot seat if they fail to take steps to oversee management's risk culture, appetite, and tolerance.

This global regulatory storm has culminated in a series of papers from the Financial Stability Board (FSB), a global regulatory advisory body formed following the onset of the global financial crisis. Its main objective is to provide guidance to national financial sector and securities regulators around the world. In its most recent paper, issued in 2014, the FSB called on national regulators to actively assess the "risk appetite framework" and "risk culture"

No. DN-V7N3
JUNE 2015
Subscribe for free at www.conference-board.org/directornotes

THE CONFERENCE BOARD
Trusted Insights for Business Worldwide

of systemically important financial institutions (SIFI), including assessing boards' effectiveness in overseeing their company's risk culture. The FSB summarized the new expectations of national financial sector regulators as follows: [4]

> "…efforts should be made by financial institutions and by supervisors to understand an institution's culture and how it affects safety and soundness. While various definitions of culture exist, supervisors are focusing on the institution's norms, attitudes and behaviour related to risk awareness, risk taking and risk management, or the institutions' risk culture."

The Financial Reporting Council (FRC), the United Kingdom's national securities regulator, reacted to the FSB's recommendations by updating The UK Corporate Governance Code that applies to all UK public companies. Provision C.2.3 of the Code mandates that the board should annually review and report on the effectiveness of their company's risk management and internal control systems. Specifically, Item 43 in Section 5 of the guidance requires the board, in its annual review of effectiveness, to consider the company's "willingness to take on risk (its 'risk appetite'), the desired culture within the company and whether this culture has been embedded."[5]

The FRC, recognizing that there is little tangible guidance available to boards on how to oversee a company's culture, stated that, in 2015, the initial year of implementation of the new board oversight requirements, it will focus on "company culture: how best to assess culture and practices and embed good corporate behaviour throughout companies."[6]

Financial regulators globally, including the SEC, are expected to follow the UK's lead and significantly increase their focus on board oversight of corporate culture generally, and risk culture in particular. In a global survey conducted by KMPG, 1,500 audit committee members ranked government regulation second among risks that pose the greatest challenge for their company.[7] Oversight of risk culture may be one of those areas of new government regulation.

The purpose of this paper is to provide board members with an overview of these new expectations and to outline potential handicaps that boards may encounter. The paper also offers suggestions for boards of directors on overseeing their company's risk culture.

Board Oversight of Risk Culture: A Primer

In a 2009 report on reform in the financial services industry, the Institute of International Finance (IIF) proposed the following definition of "risk culture":[8]

> "…norms and traditions of behaviour of individuals and of groups within an organization that determines the way in which they identify, understand, discuss, and act on the risks the organization confronts and the risks it takes."

The Financial Stability Board ("FSB") has emphasized the importance of risk culture in a number of recent guidance papers.[9] Following the consideration of feedback the FSB received to the publication in 2013 of an exposure draft on assessing risk culture, the agency issued guidance on assessing risk culture in April 2014.[10] This FSB guidance may well prove to be a turning point in the history of the evolution of regulatory supervision approaches and board risk oversight expectations.

The ongoing discussion of the role of regulators in overseeing the risk culture of financial institutions raises the question of whether national regulators are equipped to assess and opine on whether a company has a poor, adequate, good, or even the more elusive, excellent risk culture. A number of respondents to the 2013 FSB exposure draft on risk culture questioned whether regulators had the capabilities necessary to form sound, repeatable conclusions on this important issue, with particular concerns expressed that it could become a "check-the-box" exercise (see, for example comment letters issued by the US Chamber of Commerce, Professional Risk Managers International Association, and the International Actuarial Association).[11] Risk Oversight's comment letter even questioned whether global regulators were inadvertently handicapping efforts globally by encouraging companies to implement frameworks that purport to foster better risk culture by requiring binary (effective/ineffective) reports on internal control effectiveness.[12]

The April 2014 FSB guidance provides a high-level vision of what it believes represents a "sound" risk culture: [13]

> A *sound* risk culture consistently supports appropriate risk awareness, behaviours and judgments about risk taking within a strong risk governance framework. A sound risk culture bolsters effective risk management, promotes sound risk taking, and ensures that emerging risks or risk taking activities beyond the institutions risk appetite are recognized, assessed, escalated and addressed in a timely manner.

The FSB identifies risk governance, risk appetite, and compensation as the "foundational elements of a sound risk culture." While acknowledging that "assessing risk culture is complex," the FSB asks national regulators to consider the following indicators of a sound risk culture during their inspections/audits: tone from the top, accountability, effective communication and challenge, and incentives. The FSB recommends that regulators consider these indicators "collectively and as mutually reinforcing" rather than individually. Details on the risk culture indicators are shown in the box, right.[14]

The UK FRC recommends that, in conjunction with its guidance, boards, consider and discuss with senior management the following questions:[15]

- How has the board agreed the company's risk appetite? With whom has it conferred?
- How has the board assessed the company's culture? In what way does the board satisfy itself that the company has a 'speak-up' culture and that it systematically learns from past mistakes?
- How do the company's culture, code of conduct, human resource policies and performance reward systems support the business objectives and risk management and internal control systems?
- How has the board considered whether senior management promotes and communicates the desired culture and demonstrates the necessary commitment to risk management and internal control?
- How is inappropriate behaviour dealt with? Does this present consequential risks?
- How does the board ensure that it has sufficient time to consider risk, and how is that integrated with discussion on other matters for which the board is responsible?

Other regulators around the globe could follow the UK's lead by increasing their focus on risk oversight and risk culture. "Tone at the top" has been espoused by the head of the US SEC. In a July 2014 speech, SEC chair Mary Jo White noted: [16]

> Ensuring the right 'tone at the top' for a company is a critical responsibility for each director and the board collectively. Setting the standard in the boardroom that good governance and rigorous compliance are essential goes a long way in engendering a strong corporate culture throughout an organization.

Given this renewed focus on directors as gatekeepers and "tone at the top," board oversight of corporate risk culture could be an important area of SEC focus and scrutiny going forward.

Tone from the top: The board and senior management are the starting point for setting the financial institution's core values and expectations for the risk culture of the institution, and their behaviour must reflect the values being espoused. A key value that should be espoused is the expectation that staff act with integrity (doing the right thing) and promptly escalate observed non-compliance within or outside the organisation (no surprises approach). The leadership of the institution promotes, monitors, and assesses the risk culture of the financial institution; considers the impact of culture on safety and soundness; and makes changes where necessary.

Accountability: Relevant employees at all levels understand the core values of the institution and its approach to risk, are capable of performing their prescribed roles, and are aware that they are held accountable for their actions in relation to the institution's risk-taking behaviour. Staff acceptance of risk-related goals and related values is essential.

Effective communication and challenge: A sound risk culture promotes an environment of open communication and effective challenge in which decision-making processes encourage a range of views; allow for testing of current practices; stimulate a positive, critical attitude among employees; and promote an environment of open and constructive engagement.

Incentives: Performance and talent management encourage and reinforce maintenance of the financial institution's desired risk management behaviour. Financial and nonfinancial incentives support the core values and risk culture at all levels of the institution.

Source: Financial Stability Board, "Guidance on Supervisory Interaction with Financial Institutions on Risk Culture: A Framework for Assessing Risk Culture," April 7, 2014, p. 3.

Challenges for Board Oversight

1 Many board members, because of their years of real-world experience, are able to informally gauge the risk appetite and tolerance of senior management, especially CEO/CFOs, but there is very little practical guidance available on how boards should assess and document the appropriateness of the risk culture of an entire organization.

2 Senior management, including the CEO and CFO, may be reluctant to let the board know their "real" risk appetite/tolerance, as it may conflict with compensation systems and/or career advancement goals. It is now well-documented that one of the risks that boards face is "asymmetric information"[17] (the risk that management knows things about the state of risk that the board does not) when overseeing management's risk appetite and tolerance.

3 Many boards may not receive a consolidated report (like a balance sheet) on the state of retained risk across their company's top value creation and/or strategic business objectives and foundational objectives such as reliable financial reporting, compliance with laws, preventing unauthorized access to data, safety, and other social responsibility areas. A recent study indicates "only 30 percent describe their ERM process as systematic, robust, and repeatable with regular reporting of top risks to the board. That percentage is higher (55 percent) for large organizations and public companies (59 percent)".[18] Only a consolidated report on residual risk status provides a window for the board on the interrelationships between objectives and related risks that cross multiple risk and assurance silos.

4 Traditional internal audit processes and teams that provide point-in-time and subjective opinions on the effectiveness of internal controls are not well-equipped to provide boards with opinions on an organization's risk culture, the effectiveness of risk management processes, or consolidated reports on residual risk status linked to key strategic and foundation objectives.[19]

5 Risk-centric ERM processes that use risk registers that focus on identifying and assessing individual risks without linkage to related objectives and other risks impacting those objectives may not deliver concise, reliable enterprise-level information on the composite residual risk status linked to key strategic and foundation/potential value erosion objectives.[20]

6 Regulators, while increasingly calling on boards to oversee risk culture and management's risk appetite and tolerance, continue to favor the use of risk staff groups and internal audit functions as extended supervision/policing groups. This regulatory bias may handicap the efforts of progressive boards who much rather have their internal audit and risk specialists to work collaboratively with management to enhance risk processes and foster better and candid disclosure of all significant retained risk situations.

7 The regulatory and compliance regime around SOX Section 404 in the United States drives companies to build systems to report whether their "internal controls over financial reporting are effective," but stops far short of requiring that the board be told about the financial statement line items and note disclosures with highest composite uncertainty (i.e. the highest retained risk that the line items/notes may be materially wrong).[21]

8 Many ERM software applications and consulting firms continue to promote the use of risk registers and heat maps that focus on identifying and assessing individual risks, but do not provide boards with a composite picture on the residual risk status linked to key objectives.

9 Boards of directors may be relying too much on reports by the subject matter experts (including chief legal officers, chief internal auditors, heads of compliance or safety, and other assurance leaders) that state that controls are working and "effective" or "ineffective," instead of information on the highest residual risk status objectives needed to effectively monitor a company's overall risk appetite and risk culture.

10 Currently, significant confusion and debate exist on whether it is the responsibility of the full board to oversee the company's risk culture, including management's risk appetite and tolerance, or whether various board committees are individually responsible for different risk oversight functions. This may handicap efforts to create an overall picture of the company's risk culture and management's risk appetite/tolerance.

11 Although the chief audit executives of many large corporations now have a solid line relationship to the audit committee of the board, many still do not report to the board on their company's residual risk status linked to key objectives or their opinion on the company's risk culture and risk appetite framework.[22] This may be simply because their boards haven't asked for this information or because the chief audit executive doesn't know how.[23]

12 There is little practical training or guidance for board members and auditors on how to effectively oversee risk culture, including the effectiveness of risk appetite frameworks adopted by a company, from associations like the National Association of Corporate Directors (NACD) in the United States and Institute of Corporate Directors (ICD) in Canada. On the audit front, the curriculum and professional practice standards for Certified Internal Auditors (a professional designation awarded by the IIA) continue to

be heavily weighted towards training auditors to do spot-in-time internal audits that produce subjective opinions on internal control effectiveness and "control deficiencies" and "material weaknesses"; not reports on the current state of residual risk status linked to top strategic and foundational objectives. Although the Institute of Internal Auditors (IIA) is encouraging its members to transition from traditional methods to ones more aligned with the FSB expectations, real progress to date has been slow.

The Way Forward

The following recommendations aim to help corporate boards enhance risk governance at their companies.

Get educated on the new board oversight of risk culture expectations. Consultants and the Institute of Internal Auditors are following these trends closely. Boards can proactively request that subject matter experts, consulting firms, chief internal auditors, and chief risk officers provide them with briefings on board oversight of risk culture expectations and inform them on the urgency with which the local regulators, the courts, institutional investors, credit rating agencies, activist investors, and others will likely act to hold management and boards more accountable in this area. Directors of companies in the financial services sector in particular should expect regulators to quickly elevate expectations of board oversight of risk culture.

In the UK, in addition to requiring boards to make key public disclosures regarding responsibility for risk oversight and how that responsibility is discharged, starting in 2015, external auditors will also be required to confirm that nothing has come to their attention that suggests that the required representations on risk governance from board chairs regarding risk oversight practices, including board oversight of risk culture, are wrong or misleading.[24] It's uncertain whether there will be new codified regulatory expectations in this area for all publicly listed companies in the United States and Canada.

Complete a risk culture gap assessment. The criteria selected for a gap assessment will vary by business sector and by jurisdiction. For large international financial sector organizations, the FSB guidance on sound risk culture provides a high bar to assess against. Local national regulators may have adopted lower expectations in the area of risk governance that can be used as appropriate benchmark criteria for a gap assessment, unless the business case for change presented by the FSB in their "raise the bar" risk culture oversight guidance is appealing to the board.

For US public companies outside of the financial services sector, little has been codified by the SEC regarding board risk oversight requirements beyond the broad and generalized 2009 proxy disclosure requirements described in the SEC's Proxy Disclosure Enhancements rule.[25] However, public remarks by SEC commissioners in 2014 and 2015 have stressed the importance of effective board risk oversight, and may signal that more SEC codification of board risk oversight expectations may be coming.

Consider a Board & C-Suite Driven/Objective-Centric approach to ERM and Internal Audit. Traditional "risk-centric" approaches to ERM and traditional internal audit methods have not resulted in the type of risk culture oversight and risk appetite frameworks increasingly urged by regulators.[26] Radical, not incremental change is required. A Board & C-Suite Driven/Objective-Centric ERM and internal audit approach calls for active board and C-Suite involvement in overseeing the effectiveness of their organization's risk frameworks. Management, with board oversight, specify which end result objectives they want formal assurance on, the level of risk assessment rigor they think is warranted, and the level of independent assurance they want that the risk assessments are producing reliable assessments of the current state or residual risk. Appendix 1 provides an overview of the key elements of this approach. Under this approach ERM specialists work to create robust risk assessment processes capable of delivering materially reliable consolidated reports on residual risk status for senior management and the board. Internal audit groups transition from spot-in-time audits that produce subjective opinions on "control effectiveness" on a small percentage of the risk universe for the board to the expanded role envisioned by the 2013 FSB report "Principles for an Effective Risk Appetite Framework."[27] The FSB guidance calls for internal audit departments to focus on providing reports to the board on the effectiveness of the organization's entire risk management/risk appetite framework.

Regulators should consider safe harbor provisions in the area of board risk oversight. One can argue that one of the reasons that the UK has taken the lead in the area of board risk oversight is its less punitive legal system. The punitive nature of the US legal system elevates litigation risk that can sometimes come with truly effective risk assessment processes and disclosures. This has sometimes been labelled the "two-edged sword" of risk management.[28] Regulatory reforms could provide some form of safe harbor for companies and boards that, in good faith, implement risk appetite frameworks that report on the state of residual

risk linked to key strategic and foundation objectives. Until then, legal counsels must be engaged when their company's boards are informed of residual risk status information that may include evidence of illegality, contractual non-compliance, non-use of viable controls to mitigate certain risks, conscious acceptance of certain risks, and other potentially damaging information.

Hold the CEO accountable for building and maintaining effective risk appetite frameworks and providing the board with periodic consolidated reports on the company's residual risk status. A key reason that progress on implementing robust ERM systems has been slow is a lack of C-suite accountability to provide the board with consolidated enterprise reports on the current state of residual risk. The FSB guidance on effective risk appetite frameworks calls for substantially increased CEO accountability. In this regard, the FSB stated: [29]

> 4.2 The chief executive officer should:
>
> a) establish an appropriate risk appetite for the financial institution (in collaboration with the CRO and CFO) which is consistent with the institution's short- and long-term strategy, business and capital plans, risk capacity, as well as compensation programs, and aligns with supervisory expectations;
>
> b) be accountable, together with the CRO, CFO, and business lines for the integrity of the RAF, including the timely identification and escalation of breaches in risk limits and of material risk exposures;

Once the CEO is assigned responsibility for end results like those described above, he/she can decide how best to allocate specific roles to ensure his/her responsibility to provide the board with reliable information on the current residual risk status related to key objectives is fulfilled. That may entail appointing a chief risk officer or, in smaller organizations, assigning responsibility to a chief operating officer, a senior vice president, or the organization's chief internal auditor to lead efforts to implement effective entity-level risk management and risk oversight processes. The key is that the CEO should be clear that it is his/her job to ensure both the reliability of the process that produces risk status information for boards as well the reliability of the regular report to the board on the current areas of highest retained risk and the objectives impacted.

History has shown that regulator zeal is often heavily influenced by the political agenda of the day. The Sarbanes-Oxley Act of 2002 and 2010 Dodd–Frank Wall Street Reform and Consumer Protection Act are just two examples of this. Financial sector governance reform is moving ahead at full steam globally because of a continuing flow of what the SEC Chair White has termed "egregious corporate conduct." The 2008 global financial crisis and the London Interbank Offered Rate (LIBOR) and foreign-exchange rate fixing scandals, multi-billion dollar anti-money laundering settlements, and allegations that banks provided clients with tax evasion services raise big questions about the risk culture of large banks and, for their directors, questions about the effectiveness of board risk oversight. All US-listed companies are advised to monitor SEC actions in this area closely and it is likely that other countries will follow the UK's lead in this area over the next decade. Good governance is fundamentally about a country's ability to attract and grow capital and drive national growth and prosperity by maintaining fair and equitable capital markets. Effective board oversight of risk culture is now considered a key to achieving this goal.

Appendix

Board & C-suite Driven/Objective-centric ERM: Core Elements

Core element #1 Use an objectives register Use an end-result OBJECTIVES REGISTER as the foundation building block for all ERM and assurance work done by the board, senior management, work units, internal audit, ERM teams, safety, compliance, environment and other assurance groups. This simple step elevates two core reasons for using ERM: 1) to increase the certainty that important objectives will be achieved operating within a level of residual risk status acceptable to senior management and the board, and 2) to provide reliable information to help boards and senior management make better resource allocation decisions.

Core element #2 Active board/senior management involvement and cost/benefit analysis The OBJECTIVES REGISTER should, at a minimum, include the organization's top value creation/strategic objectives and the top potential value erosion objectives (i.e. objectives where non-achievement significantly erodes entity value). This ensures that ERM integrates with strategic planning, performance evaluation and remuneration, as well as key safety, compliance and IT security initiatives. ERM and related formal assurance work consume time and money. Senior management and the board should play an active role defining which end-result objectives warrant the time and resources formal risk management requires and how much. The OBJECTIVES REGISTER plays a key role in fostering better board/C-suite-driven assurance. This simple step has great potential to integrate the work of all of the "assurance silos" and increase board risk oversight transparency.

Core element #3 Clear accountability Traditional ERM methods often focus on identifying RISK OWNERS for each risk. This approach calls for identification of an OWNER/SPONSOR for each objective selected for inclusion in the OBJECTIVES REGISTER. An objective OWNER/SPONSOR may, or may not, decide that it makes sense to assign RISK OWNERS for some or all of the significant risks that increase uncertainty a specific objective will be achieved. However the OWNER/SPONSOR retains overall responsibility for reporting upwards on RESIDUAL RISK STATUS linked to their business objective(s), not just the status of individual risks covered in more traditional risk registers. A key question that should be asked is, "Why would we assign 'risk owners' if there is no clarity/visibility on who owns and/or has responsibility for the related end result business objective?"

Core element #4 Define risk assessment rigor and independent assurance levels For each objective included in the OBJECTIVES REGISTER a RISK OVERSIGHT COMMITTEE comprised of senior management, with board oversight, should define how much risk assessment rigor and the amount/intensity of independent assurance senior management and the board believe is warranted. These decisions provide a clear roadmap for the ERM team, internal audit, and other assurance providers.

Core element #5 Consider the full range of risk treatments Properly applied, ERM should identify and assess the full range or risk treatments, including risk financing/insurance, risk transfer/sharing/contractual indemnities, risk avoidance options; as well as risk mitigation techniques, often more narrowly referenced as "internal controls." This requires input from auditors, insurance specialists, legal advisors, line management, senior management, and the board. Sometimes the best way to treat a risk is to change the objective, which may even mean exiting the business sector. Many risk-centric approaches that use risk registers do not identify the full range of risk treatments; instead they focus primarily on "internal controls." This can produce dangerous and wrong conclusions on acceptability of residual risk.

Core element #6 Focus on acceptability of composite residual risk status The objective-centric approach to ERM and internal audit produces a composite set of information called Residual Risk Status for each objective. This includes details on current and past objective performance, impact of not achieving the objective (as opposed to impact(s) linked to a single risk), any impediments that create barriers for the objective owner/sponsor to adjust residual risk status, and "concerns"—situations where a viable risk is not being treated in whole or in part. Concern data can also include information on viable risk treatments not currently in use/place that could further reduce residual risk status. Owner/Sponsors, senior management and the board use this information to help assess the acceptability of the current residual risk status. This information provides a tangible basis for identifying an organization's real risk appetite/tolerance and better allocating resources.

Core element #7 Optimize risk treatments Once a decision has been made by the OWNER/SPONSOR with oversight from senior management and the board on the acceptability of residual risk status, the entity can consider whether the current combination of risk treatments is "optimized" – i.e. the lowest cost possible combination of risk treatments capable of producing an acceptable residual risk status. Traditional ERM methods may not emphasize evaluating risk treatment optimization/cost reduction opportunities. Risk-centric processes driven by risk registers make this step difficult as the full range or risks that impact the certainty specific objectives will be achieved are not identified and evaluated in composite and the full range of risk treatments available is not considered.

Board & C-suite-driven/Objective-centric ERM Primary Ratings Definitions

Composite Residual Risk Rating Definitions

0 Fully Acceptable Composite residual risk status is acceptable. No changes to risk treatment strategy required at this time. (NOTE: this could mean that one or more significant risks are being accepted. Information on accepted concerns is found in the Residual Risk Status information).

1 Low Inaction could result in very minor negative impacts. Ad hoc attention may be required to adjust composite residual risk status to an acceptable level.

2 Minor Inaction or unacceptable terms could result in minor negative impacts. Routine management attention may be required to adjust composite residual risk status to an acceptable level.

3 Moderate Inaction could result in or allow continuation of mid-level negative impacts. Moderate senior management effort required to adjust composite residual risk status to an acceptable level.

4 Advanced Inaction could allow continuation of/or exposure to serious negative impacts. Senior management attention required to adjust composite residual risk status.

5 Significant Inaction could result in or allow continuation of very serious entity level negative impacts. Senior management attention urgently required to adjust composite residual risk status to an acceptable level.

6 Major Inaction could result in or allow continuation of very major entity level negative consequences. Analysis and corrective action to adjust composite residual risk status required immediately.

7 Critical Inaction virtually certain to result in or allow continuation of very major entity level negative consequences. Analysis and corrective action to adjust composite residual risk status required immediately.

8 Severe Inaction virtually certain to result in or allow continuation of very severe negative impacts. Senior management/board level attention urgently required to adjust composite residual risk status.

9 Catastrophic Inaction could result in or allow the continuation of catastrophic proportion impacts. Senior management/board level attention urgently required to adjust composite residual risk status and avert a catastrophic negative impact on the organization.

10 Terminal The current composite residual risk status is already extremely material and negative and having disastrous impact on the organization. Immediate top priority action from the board and senior management required to prevent the demise of the entity.

Risk Assessment Rigour ("RAR") Levels

RAR	Description
Not Assigned (NA)	Accountability to report on the Composite Residual Risk Rating ("CRRR") has not been assigned to an OWNER/SPONSOR(s)
Not Assigned (NA)	Accountability has been assigned to an OWNER/SPONSOR(s) but no CRRR has been assigned yet
Not Rated (NR)	Accountability to report CRRR status has been assigned and a CRRR rating with a brief narrative explaining the basis for the CRRR provided by the objective OWNER/SPONSOR(s) within the past 12 months
Very Low (VL)	A time-limited effort has been made to develop or update a list of risks/threats to achievement and assign RED/AMBER/GREENS to each risk within the past 12 months. Action items for all RED rated risks will be developed
Low (L)	More effort has been spent to quality assure that all significant risks have been identified using a variety of risk identification methods and the risk treatments in place/use for all, or some, of the risks have been identified and documented. Performance and impact information for the objective has been obtained and documented. Data has been updated within the past 12 months.
Medium (M)	A range of techniques have been used to identify all significant risks. Risk treatments for significant risks have been identified and efforts made to independently validate the existence and effectiveness of the risk treatments. Efforts have been made to validate the adequacy and accuracy of the linked objective performance and impact information.
High (H)	All standard RiskStatusline™ information elements have been identified and documented and additional efforts made by the OWNER/SPONSOR(s) to validate their completeness and reliability.
Very High (VH)	In addition to identifying and documenting all standard RiskStatusline™ data elements, more advanced techniques to determine velocity of risks, leading/lagging risk indicators, steps taken to assess the reliability of likelihood and consequence ratings and other advanced risk assessment techniques

Endnotes

1 See Jon Talotta, Michelle Kisloff, and Christopher Pickens, "Data Breaches Hit the Board Room: How to Address Claims Against Directors and Officers," January 23, 2015 (http://www.hldataprotection.com/2015/01/articles/cybersecurity-data-breaches/data-breaches-hit-the-board-room/).

2 Talotta, Kisloff, and Pickens, "Data Breaches Hit the Board Room."

3 United States Senate Report 107-70, "Report Prepared by the Permanent Subcommittee on Investigations of the Committee on Governmental Affairs," July 8, 2002, 107th Congress, 2d Session (http://www.gpo.gov/fdsys/pkg/CPRT-107SPRT80393/pdf/CPRT-107SPRT80393.pdf).

4 Financial Stability Board, "Guidance on Supervisory Interaction with Financial Institutions on Risk Culture: A Framework for Assessing Risk Culture," April 7, 2014, p.1 (http://www.financialstabilityboard.org/wp-content/uploads/140407.pdf?page_moved=1).

5 Financial Reporting Council, "Guidance on Risk Management, Internal Control and Related Financial and Business Reporting," September 2014 (https://www.frc.org.uk/Our-Work/Publications/Corporate-Governance/Guidance-on-Risk-Management,-Internal-Control-and.pdf).

6 Financial Reporting Council, "Developments in Corporate Governance and Stewardship 2014," January 2015, p. 23 (www.frc.org.uk/Our-Work/Publications/Corporate-Governance/Developments-in-Corporate-Governance-and-Stewardsh.pdf).

7 2015 Global Audit Committee Survey, KPMG's Audit Committee Institute (http://www.audit-committee-institute.be/dbfetch/52616e646f6d495677657b7b3a3cd8e673d6626bead407d0/2015-global-audit-committee-survey.pdf).

8 Institute of International Finance, "Reform in the Financial Services Industry: Strengthening Practices for a More Stable System." December 2009, p. AIII.2 (www.iif.com/file/7071/download?token=w6PvaJA3).

9 See, for example "Principles for an Effective Risk Appetite Framework," Consultative Document, July 17, 2013 (http://www.financialstabilityboard.org/wp-content/uploads/r_130717.pdf).

10 Financial Stability Board, "Guidance on Supervisory Interaction with Financial Institutions on Risk Culture," p. 1.

11 Responses to the FSB exposure draft on assessing risk culture can be found at (http://www.financialstabilityboard.org/2014/02/c_140206/).

12 See Risk Oversight response letter to FSB dated January 14, 2014 (http://www.financialstabilityboard.org/wp-content/uploads/c_140206u.pdf).

13 Financial Stability Board, "Guidance on Supervisory Interaction with Financial Institutions on Risk Culture," p. 1.

14 Financial Stability Board, "Guidance on Supervisory Interaction with Financial Institutions on Risk Culture."

15 Financial Reporting Council, "Guidance on Risk Management, Internal Control and Related Financial and Business Reporting," p. 21.

16 "A Few Things Directors Should Know About the SEC," SEC Chair Mary Jo White to the Stanford University Rock Center for Corporate Governance Twentieth Annual Stanford Directors' College, June 23, 2014 (http://www.sec.gov/News/Speech/Detail/Speech/1370542148863#.VQs7KxCZhqY).

17 See NACD BoardVision: Asymmetric Information Risk, National Association of Corporate Directors, March 28, 2013 (https://www.nacdonline.org/Resources/BoardVisionEpisode.cfm?ItemNumber=6668).

18 Mark Beasley, Bruce Branson, and Bonnie Hancock, "2015 Report on the Current State of Enterprise Risk Oversight: Update on Trends and Opportunities," February 2015, p. 3 (http://erm.ncsu.edu/az/erm/i/chan/library/AICPA_ERM_Research_Study_2015.pdf).

19 See Tim J. Leech, "Reinventing Internal Audit," *Internal Auditor*, April 2015 for more details.

20 See Tim Leech, "The High Cost of ERM Herd Mentality: Why Traditional Approaches Have Failed," white paper, March 2012 (http://riskoversightsolutions.com/wp-content/uploads/2011/03/Risk_Oversight-The_High_Cost_of_ERM_Herd_Mentality_March_2012_Final.pdf).

21 See Leech, "Reinventing Internal Audit."

22 See Leech, "Reinventing Internal Audit."

23 See Leech, "Reinventing Internal Audit."

24 International Standard on Auditing (UK and Ireland) 700: The independent auditor`s report on financial statements, Financial Reporting Council, June 2013, paragraph 22, p. 8.

25 SEC Final Rule, Proxy Disclosure Enhancements, effective February 28, 2010 (https://www.sec.gov/rules/final/2009/33-9089.pdf).

26 See Leech, "Reinventing Internal Audit."

27 Financial Stability Board, Principles for an Effective Risk Appetite Framework, November 18, 2013 (http://www.financialstabilityboard.org/wp-content/uploads/r_131118.pdf?page_moved=1).

28 See Parveen P. Gupta and Tim J. Leech, "Risk Oversight: Evolving Expectations for Boards," The Conference Board, *Director Notes*, DNV6N1, January 2014, p. 7.

29 Financial Stability Board, Principles for an Effective Risk Appetite Framework, p. 9.

About the Authors

Parveen P. Gupta is the Clayton Distinguished professor of accounting and the department chair 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 at Risk Oversight Solutions Inc. headquartered in Oakville, Ontario, Canada. 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" and co-authored "Risk Oversight: Evolving Expectations for Boards." Tim's most recent article, "Reinventing Internal Audit" published by the IIA in the April issue of Internal Auditor, has received global recognition and accolades. He lives in Oakville, Ontario, with Elaine, his wife for over 39 eventful years and has two daughters, Lauren and Morgan, and, most recently his first granddaughter.

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 *U.S. Directors' Compensation and Board Practices* and *Institutional Investment reports,* and *Sustainability in the Boardrooom*. 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,* an 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 co-author 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.

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