Conference Board Director Notes

Board Oversight of Management’s Risk Appetite and Tolerance: Utopian Fantasy or Stretch Objective?

by Parveen P. Gupta and Tim J. Leech

Regulators around the world are increasingly calling for board oversight of management’s risk appetite and tolerance. Their goal in holding the directors more accountable for risk oversight is simple - prevent yet another wave of massive corporate governance meltdowns with catastrophic impact on stakeholder value. This Director Notes takes a hard look at whether this regulatory goal is a “utopian fantasy”, virtually impossible to achieve in real life, or more akin to a “stretch objective” – difficult but possible when there is genuine will to achieve it.

About the Authors
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, Europe, Australia, South America, Africa, the Middle East and Asia. Tim and his daughter Lauren co-authored 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”. Most recently, he authored and published a Conference Board Director Notes paper in December 2012 titled, “Board Oversight of Management’s Risk Appetite and Tolerance”. He lives in Oakville, Ontario, with Elaine, his wife for over 38 eventful years.

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 a recipient of many awards in teaching and research. During 2006-07, he served as an Academic Accounting Fellow in the Division of Corporation Finance at the SEC. There 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

---

1 We would like to thank the following individuals for reviewing and providing feedback on earlier versions of this paper: 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 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. All views expressed are entirely those of the authors.

2 For purposes of this paper 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)
industry clients and Big-4 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 media.

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, Sustainability in the Boardroom, and the forthcoming Risk Oversight Handbook. 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 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 non-advocacy, not-for-profit entity, holding 501(c) (3) tax-exempt status in the United States.
Board Oversight of Management’s Risk Appetite & Tolerance: Utopian Fantasy or a Stretch Objective?

The 2008 global financial crisis was a jolt to regulators and elected government officials responsible for ensuring safety and stability of global capital markets. The enormity of the global economic meltdown and the ensuing global recession, accompanied by unprecedented bailouts of public companies around the world, made it absolutely clear to all that risk governance frameworks had failed miserably. A plethora of Commissions and Special Inquiries were launched globally to try to answer the obvious questions – What went wrong? Why had risk management systems failed? Where were the Boards of Directors?

One of most comprehensive and in-depth evaluations was undertaken by the highly influential Senior Supervisors Group (SSG) - a forum comprising financial regulators from Canada, France, Germany, Japan, Switzerland, the United Kingdom, and the United States. The SSG, a forum largely unnoticed by the global business community, published two separate and informative reports addressing the key question “what went wrong?” In the transmittal letter accompanying the second report, the group summarized a number of areas of weakness they felt required further work:

- 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.

The Senior Supervisors’ conclusions led to calls for a significant increase in the involvement of the board of directors in risk governance, specifically the role of boards overseeing management’s risk appetite and tolerance, more particularly “bet the farm” type risks. Even greater regulatory focus and action in this area is expected in the years ahead.

In this Director Notes we don’t attempt to deal with all aspects of the management of the effects of uncertainty on achievement of business objectives as that would require a full-length article or perhaps even a book. This Director’s Notes focuses on more modest objectives - alert boards of directors to rising expectations from a range of key players linked to “board oversight of management’s risk appetite and tolerance” and “risk management”; analyze major impediments

---


5 NOTE: the term “risk appetite and tolerance” is evolving. The July 2013 FSB paper “Principles for an Effective Risk Appetite Framework” on page 2 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”.

---

3
that even the most well-intending boards face today in meeting these rising expectations; and propose what may appear radical but is in fact a relatively simple approach – board-driven, objective-centric risk governance. The central notion of this approach is that boards should be demanding information regularly from management generally, and CEOs in particular, on the state of residual/retained risk status linked to key objectives. Internal audit or another independent provider should provide assurance on the reliability of the risk status information the board receives. While exploring current pervasive and daunting handicaps to this relatively new and escalating Board imperative, this Directors Note raises, by extension, another key question that has largely escaped attention: Are the calls for board oversight of management’s risk appetite and tolerance a utopian fantasy, virtually impossible to achieve in real life, or more akin to a stretch objective - difficult but possible when there is genuine resolve to achieve it.

The Rising Expectations

In the aftermath of the 2008 global financial crisis calls to hold boards more accountable for effective oversight of a company’s risk appetite and tolerance are coming from all quarters. Based on the small sample of influential expectations summarized in this paper, it is virtually certain that board risk oversight expectations will continue to rise.

*The National Association of Corporate Directors (NACD)*

Shortly after the 2008 global financial crisis began, as a preemptive strike to ward-off Sarbanes-Oxley like legislation and ensuing regulatory backlash, the NACD assembled a “Blue Ribbon Commission”. The Commission issued an insightful and forward-looking report in 2009, *Risk Governance: Balancing Risk and Return*, to tackle the issue head-on. The Commission’s report makes six key recommendations:

While risk oversight objectives may vary from company to company, every board should be certain that:

- the risk appetite implicit in the company’s business model, strategy, and execution is appropriate;
- the expected risks are commensurate with the expected rewards;
- 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;
- the risk management system informs the board of the major risks facing the company;
- an appropriate culture of risk-awareness exists throughout the organization;
- there is recognition that management of risk is essential to the successful execution of the company’s strategy” (NACD, 2009, p.4)

Although these recommendations may appear obvious, even simplistic to some readers, putting them into practice is a clear reminder that often “the devil is in the details”.

---


**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 deal with their oversight responsibilities. While discussing board’s role in the risk management, the report notes that

> 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 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 (Tonello, 2009, p. 13)⁷

**U.S. Securities and Exchange Commission (SEC)**

The SEC reacted to the findings and recommendations of the two SSG Reports by issuing Final Rules that required enhanced proxy disclosures from all U.S. listed public companies. The Final Rules (SEC Release Nos. 33-9089 and 34-61175) effective February 28, 2010 notes 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 (p. 44)”⁸

Emphasizing the relevance of disclosing details on a board’s oversight of a company’s risk management framework SEC Commissioner Louis Aguilar more recently noted that:

> Item 407(h) also requires companies to describe the role of the board of directors in the oversight of risk… Given the magnitude of [the] 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 engage⁹

---


⁹ United States Securities and Exchange Commission, Public Statement by Commissioner Luis A. Aguilar, Shareholders Need Robust Disclosures to Exercise Their Voting Rights as Investors and Owners, SEC, Washington,
In spite of this outwardly strident SEC stance from one Commissioner, it remains to be seen whether the Commission will further strengthen risk oversight disclosure rules and visibly sanction registrants that provide non-compliant, uninformative, and boilerplate disclosures.

**Dodd-Frank Wall Street Reform and Consumer Protection Act**

The U.S. Congress responded to the 2008 financial crisis by enacting the Dodd-Frank Wall Street Reform and Consumer Protection Act on July 21, 2010. Among a number of other measures to rein-in the moral hazard, too big to fail, risk-taking demonstrated by global financial institutions, Section 165(h)\(^{10}\) of the Act requires certain public companies subject to Federal Reserve jurisdiction to establish a board-level risk committee specifically responsible for the oversight of a company’s enterprise-wide risk management practices.

**International Corporate Governance Network (ICGN)**

The International Corporate Governance Network (ICGN) “represents investors, companies, financial intermediaries…and others interested in the development of global corporate governance practices” (2010, p. 4). In 2010, this influential group issued ICGN Corporate Risk Oversight Guidelines with the objective of helping investors assess the effectiveness of a company’s board overseeing risk management.

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 (2010, p. 5). With regard to corporate risk oversight, the ICGN guidelines unambiguously note 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 (2010, p. 8).\(^ {11} \)

**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. It achieves this goal by bringing together 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*, from a survey of its 24 member countries. Based on its review, one of the key recommendations is that member countries “should strengthen their regulatory and supervisory guidance…to assess the effectiveness of risk governance frameworks” (2013, p. 4). More specifically, it recommends that boards of directors be held

…accountable for its 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. 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 (2013, p. 4).\(^\text{12}\)

The report was followed by the release of an FSB Consultative Document, *Principles for an Effective Risk Appetite Framework*, in July 2013 which proposes 12 specific, what some may even term “utopian,” board expectations listed below:

a) approve the firm’s RAF [risk appetite framework], developed in collaboration with the CEO, CRO and CFO, and ensure it remains consistent with the firm’s short- and long-term strategy, business and capital plans, risk capacity as well as compensation programs;

b) 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;

c) ensure that annual business plans are in line with the approved risk appetite and incentives/disincentives are included in the compensation programmes to facilitate adherence to risk appetite;

d) include an assessment of risk appetite in their strategic discussions including decisions regarding mergers, acquisitions, and growth in business lines or products;

e) 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;

f) discuss and determine actions to be taken, if any, regarding “breaches” in risk limits;

g) question senior management regarding activities outside the board-approved risk appetite statement, if any;

h) 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;

i) 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;

j) 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;

k) 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

l) ensure risk management is supported by adequate and robust IT and MIS to enable identification, measurement, assessment and reporting of risk in a timely and accurate manner.\(^\text{13}\)

The board risk oversight developments noted above represent only a small fraction of the global movement to hold the boards more accountable for setting and overseeing management’s risk appetite and risk tolerance and related supporting frameworks. In spite of the rapid escalation in expectations, what has not received sufficient attention to date is recognition that, at the current time, even the most expert, diligent and well-meaning boards face major impediments to faithfully discharging these new fiduciary responsibilities.

**Handicaps to Effective Board Oversight of Risk**

*Asymmetric Information – What the board doesn’t know can hurt them*

Following the issuance of their 2009 Blue Ribbon Commission Report the NACD recognized that transformational changes in board composition, attitudes, and behavior require focused and concerted effort. In 2012, the NACD, with the support of PwC and Gibson Dunn, formed a new Advisory Council specifically on Risk Oversight to identify and elevate leading risk oversight practices. The Council has four specific stated goals

- Discuss ways the board can get engaged in addressing risk areas
- Highlight the practices and processes the board should focus on
- Develop more precise definitions of risk oversight practices
- Identify the resources needed to effectively engage in those practices\(^\text{14}\)

---

\(^{13}\) Principles for An Effective Risk Appetite Framework Consultative Document, Financial Stability Board, July 2013, page 7

One of the key conclusions from Council’s deliberations to date is that asymmetric information risk - where the management has more and better information than the directors - presents a real challenge for the boards. In this regard, the Advisory Council noted:

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 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.\(^\text{15}\)

The existence of asymmetric information was boldly highlighted in a January 14, 2008 Wall Street Journal Report on Corporate Governance which concluded that the CEOs need to be honest with their boards and not “sugarcoat” the truth. The excerpt below highlights the need for honest communication and transparency between the senior management and their board:

As a former chief executive officer of Gillete Co. and Nabisco Inc., James M. Kilts knows a thing or two about dealing with corporate boards. So, when Mr. Kilts gave a keynote speech at a corporate-governance conference last April, he decided to share some of what he has learned over the years. The advice was surprisingly simple. “Tell the truth,” Mr. Kilts told the crowd of executives, directors, corporate-governance gurus and others. CEOs, he said, must be open with their board about a range of issues, from the failure of strategic plans to unsavory business practices.

\(^\text{16}\)Lack of Consensus: What Does “Overseeing Management's Risk Appetite & Tolerance” Really Mean?

As the global regulatory spotlight increasingly turns to board risk oversight, so too have efforts to build consensus on what the terms “risk appetite” and “risk tolerance” mean in practice. To gain a sense of the plethora of views, one only needs to search the terms on Google. As of August 2013, googling the terms yielded a staggering 782,000 results. According to Jim DeLoach, a recognized authority in the risk field, a common language is an essential starting point for effective enterprise-


wide risk management. It enables communication, promotes learning, facilitates aggregation, and is the fundamental building block of an organization’s risk management program and processes.\(^{17}\)

Building a consensus around what “board oversight of management’s risk appetite and tolerance” really means in practice is an important step towards developing practical “how to” strategies. Some even argue that before we delve into reforming board risk oversight, we need to clearly articulate with great specificity what we mean by terms “risk appetite” and “risk tolerance.” We recommend that influential organizations and regulatory bodies mentioned earlier undertake a joint effort to provide clarity on these terms in the interest of developing “common-language.”\(^{18}\)

Even after significantly increased attention, our sense is that board understanding of “how to really do it in real life” continues to be at an embryonic stage. For example, it is unlikely that many boards of the companies involved in the 2008 financial crisis and other recent governance failures linked to Foreign Corrupt Practices Act (“FCPA”) violations, anti-money laundering transgressions, fraudulent financial statements, devastating environmental events, and other catastrophes asked their CEO and the senior management team direct and pointed questions such as:

- When making these investments how did you decide what the company’s tolerance was to financial instruments whose safety was premised on the assumption that the U.S. real estate market would continue to rise indefinitely?
- How did you determine company’s tolerance to violating laws and regulations?
- How did you determine that violating the Foreign Corrupt Practices Act of 1977 was within company’s risk appetite and tolerance?
- How did you decide how much money laundering was/is within company’s risk appetite and tolerance?
- Do you know what our risk tolerance criteria are for 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’s injuries and fatalities?
- How do you (senior management) decide how many seriously dissatisfied customers are acceptable?
- How do you decide on the acceptable level of defective, potentially dangerous products we (the board and senior management) are prepared to tolerate?
- 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 in areas where compensation systems may cause generally good employees to commit illegal/unethical acts?

---


\(^{18}\) We don’t pretend to provide these definitions but can analogize risk appetite to “eyes” meaning willingness to take risks and risk tolerance to the “stomach” meaning ability to handle the adverse outcome.
Majority of ERM Frameworks Today Provide Limited and Generally Poor Quality Information on Management’s Risk Appetite/Tolerance

Boards are being asked to ensure that there are effective risk management frameworks in place to allow them to oversee management’s risk appetite and tolerance. Unfortunately, a large percentage of efforts to implement what is commonly called Enterprise Risk Management (“ERM”) have been done using what is best termed a “risk centric” approach where the focus is on “risks”, without equal or greater focus ensuring clear linkage to related end result business “objectives”. Generally this approach involves running annual workshops and/or asking management via interviews and/or on-line surveys what they see as the biggest risks. This “annual update” generates lists of top 10, top 20, top 50 risks together with any action plans to address “red rated” risks. 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, as amazing as it may seem, we believe that only a minority of risk management frameworks in use today require formal risk assessments on 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. This observation is supported in whole or part by a range of surveys conducted around the world over the past three years. The linkage between the risks periodically reported to the board and the objectives most key to the long term success of the company are frequently opaque at best, totally non-existent at worst.

In most cases the risk centric approach in use in the majority of organizations around the globe 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 (e.g. objectives like ensure all laws in all jurisdictions the company operates are complied with, increase the company’s market share by 10% year over year). Risk centric approaches, in addition to focusing on risks in isolation, often do not formally enumerate the full range of risk treatments in place for the identified fragmented risks. When attempts are made to identify linked risk treatments, the focus is often on documenting only what is generally broadly known as “internal controls”. Risk transfer, risk financing, risk sharing, risk avoidance, and risk acceptance vehicles, even when they are key to the real corporate risk treatment strategy, are often not formally considered or included in the risk information presented to boards. Even for the most important, high visibility business objectives, 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. What hasn’t been selected to treat/mitigate key risks is often as relevant to
decision makers as what has been chosen.

**Traditional Internal Audit Approaches Provide Subjective Opinions on Control Effectiveness,
Not Valuable Information for Decision Making on Entity Wide Residual/Retained Risk Status**

Traditional “direct report” approaches to internal audit (approaches where internal auditors function as the primary formal risk/control analysts/reporters) call on the chief internal audit executive to use, what is often loosely referred to as, a “risk-based” audit approach. Our experience indicates that internal auditors when performing their “risk assessments” rarely utilize risk assessment methods advocated by global standard setters like ISO 31000. Often, based on some arbitrary factors, decisions are made on a number of topics, business areas, or issues to include in the upcoming audit cycle for conducting point-in-time audits. In the next step, based on their budget or management’s priorities, some percentage of the audits chosen are completed and results of those point-in-time audits reported upwards to senior management and sometimes the organization’s audit committee. The coverage of these point-in-time assessments as a percentage of an organization’s total risk universe is usually a very small percentage of the total risk universe.

Visually Figure 1 captures typical internal audit coverage. In addition to serious coverage limitations and auditor subjectivity on what constitutes “effective” control, the level of rigor used to assess areas selected by internal audit varies enormously. Boards are often not informed which areas/topics were rigorously assessed and which ones received only cursory attention.

**FIGURE 1**

<table>
<thead>
<tr>
<th>Typical Annual Coverage of Full Risk Universe</th>
<th>Typical Board Deliverable</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Typical Annual Coverage of Full Risk Universe" /></td>
<td>1. Some number of audit reports.</td>
</tr>
<tr>
<td></td>
<td>2. Annual broad summary observations from the head of internal audit based on audits completed during the past year.</td>
</tr>
<tr>
<td></td>
<td>3. Details on which units have not agreed to implement audit recommendations may or may not be provided to the board.</td>
</tr>
<tr>
<td></td>
<td>4. Special review reports.</td>
</tr>
</tbody>
</table>

In most organizations today internal auditors still focus on assessing whether, “in their professional opinion” they believe internal controls are “effective”. They often render these opinions in the absence of any clear indication of what level and types of retained/residual risk are acceptable to

---

senior management and the board of directors. Approaches used to complete the audits are often a combination of a myriad of approaches such as testing for compliance with policies; testing “key internal controls” as auditors deem fit; evaluating business processes, or assessing whether the organization manifests the attributes of a particular control framework such as the legacy COSO 1992 control framework. Unfortunately, these methods do not provide boards with the breadth and depth of information necessary to effectively oversee management’s risk appetite and tolerance. The 2008 global financial crisis is a case in point supporting this observation – based on publicly available information few, if any, internal audit departments in the suspect companies alerted their boards to the massive retained risk levels being accepted by their management.

Credit Rating Agencies and Boards Still Not Sure What Effective Risk Governance Looks Like

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” as a key obstacle to adequately assessing credit risk exposures.

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

Litigation Risk: Knowing Management’s Real Risk Appetite/Tolerance Potentially Dangerous to Boards

Truly effective risk management provides transparency and disclosure when decisions are made to consciously accept risks. In many cases formal risk management elevates unconscious decision-making to conscious decision-making – a key element when things go badly wrong establishing what is known in law as “mens rea or a guilty mind”. A lack of knowledge on the part of boards on management’s true risk appetite and tolerance creates the tangible benefit of, what former President Nixon referred to during the Watergate Scandal, as “plausible deniability” or, stated another way “ignorance is bliss”.

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 but the point here is not just to comply with the IIA 2120 Standard but it is to assure the boards that the residual risk status of the company is within the risk appetite and tolerance set by them
Unfortunately, in some instances, major risks sometimes do materialize and result in severe negative consequences. Risks which can, in severe cases, result in the complete demise of an entity. In litigious societies, particularly the U.S., knowledge of a risk acceptance decision by senior management and sometimes the board, when in the possession of a regulator, criminal prosecutor, or plaintiffs’ bar armed with the benefit of 20-20 hindsight, can significantly increase personal and corporate legal exposure. This litigation risk needs to be carefully weighed against the possibility that not formally assessing and managing risks can be seen by regulators and the courts as negligent, or even breach of management’s and board’s fiduciary duty of care. This conundrum, referred to as “the two-edged sword of risk management” or more colloquially “damned if we do and damned if we don’t” needs to be understood and carefully considered.

The good news for boards is that the Delaware Chancery Court, to-date, has been reluctant to hold boards to a very high standard of risk oversight. To substantiate this apparent bias, Harner (2010) notes that:

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.”

Boards Simply Haven’t Asked Management for the Type of Information They Need

Last but certainly not least, 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. A large percentage of boards, for a variety of reasons, including the ever popular “this is how we’ve always done it” rationale, have simply not asked the senior management and other relevant parties for the type, quality, and quantity of information necessary for them to discharge the new risk governance expectations. Change needs to start with a key question: Who has the real control of the agenda for board meetings and is the board meaningfully influencing the type and quantity of retained risk status information they get from management, internal auditors, risk functions, Chief Legal Counsel, external auditors, and other key players?

The Way Forward: Board/Demand Driven/Objective-Centric Risk Governance

The list of pervasive and potentially disabling handicaps outlined in the previous section represents major impediments for even the most diligent, well-intending boards who want better risk

---

oversight processes and information. The army of consultants focused on providing advice to boards and helping organizations respond to the new risk oversight expectations is growing rapidly. Unfortunately, many of the consultants are selling “old wine in new bottles” by promoting “same old/same old” internal audit and ERM solutions repackaged to meet new board risk oversight expectations.

In this section we offer eight specific recommendations based on 25+ years of global ERM experience that we believe, using a compass analogy, point to “true north” to help boards that truly want to meet the new board risk oversight expectations.

Recommendation #1: Transform the risk management and the 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 and, more recently, from the ERM function when one exists. These assurance providers, for the most part, have been “supply-driven”, largely making their own decisions on what their customers, including boards of directors and senior management, want from them to discharge their fiduciary responsibilities. As long as board risk oversight expectations were low, the deficiencies of the status quo in internal and external audit and ERM practices were, for the most part, tolerated by busy boards. The rapid emergence of globally codified board risk oversight expectations dictates that board tolerance for low quality risk status information from these assurance providers must change, and change rapidly, if boards are to be assured that they are aligned with new risk oversight expectations.

Boards need to “demand” reliable risk management and risk oversight processes, and formal written opinions on their effectiveness from independent and qualified assurance providers. This simple step of boards demanding better risk governance processes, processes capable of ensuring boards meet the new risk oversight expectations, has great potential to revolutionize practices globally.

Recommendation #2: Clarify Accountabilities

A key step to mobilize all the players that must contribute to meeting the new risk governance expectations is to actively discuss the new board risk oversight expectations at the board level; decide which expectations are most relevant to the organization; and agree on a corporate strategy to meet them. A simple way to get started is to agree core end results expected from each risk governance participant and document them. Attachment 1 to this Director Note provides a sample “Board/Demand driven/Objective Centric” risk governance policy, including suggested accountabilities for the board, CEOs, senior management, work units, and specialist assurance groups. It’s important to note that boards that elect, consciously or unconsciously, to continue to tolerate ineffective risk management and risk oversight practices and processes need to be aware that they are now making a very significant, and increasingly “risky”, risk acceptance decision.

Recommendation #3: Put the focus on end result objectives

ISO 31000, the most globally accepted risk management standard, defines risk as the “effect of uncertainty on objectives.” Unfortunately, a large percentage of the risk and control work done today around the globe loses the visible linkage between risks and end result objectives, and often does not focus resources on assessing the risks to the objectives most key to value creation, and surprisingly, objectives with the highest statistical probability of eroding entity value. We recommend that 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 employ an “objective-centric” risk assessment process that actively supports the straightforward ISO 31000 risk definition.

Attachment 2 provides an example of an objective-centric risk assessment approach. A key feature of this approach, a feature which is not currently part of ISO 31000, is that it 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 non-achievement of the objective in whole or part. It’s important to note that this approach is quite different from traditional ERM methods that assess the range of likelihood and impact of a single risk and risks in isolation. This approach has been specifically designed to assist management and boards decide if the current retained risk position linked to key value creation and potentially value eroding objectives is, or is not, 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, consciously or unconsciously.

Another unique feature is that 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,” where optimized means the lowest cost risk treatment strategy capable of producing an acceptable level of retained risk. Few boards in the world today receive much information, if any, on whether risk treatments are optimized from internal audit or ERM support functions.

Recommendation #4: Change Internal Audit’s Mandate and Reporting Relationships in the Organizational Hierarchy

In a large percentage of organizations today the primary mandate of internal audit is to plan audits, complete audits, 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, or ineffective, without the benefit of truly knowing senior management and the board’s risk appetite and tolerance. Management in the areas selected for traditional direct report audits is often under significant pressure to remediate unmitigated risks identified by internal audit, regardless of whether there are other areas not included in internal audit’s relatively tiny annual coverage 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 sub-optimal and distorted misallocation of corporate resources. This distortion of rational resource allocation can be amplified by well-intending boards that believe part of their job is to ensure that internal audit findings and recommendations are addressed by management.

A far better and more useful mandate for an internal audit function is to assess and report on the effectiveness of an organization’s risk management processes (or as is increasingly being referred to as an organization’s “Risk Appetite Framework”), and the reliability of the consolidated reports on the organization’s overall risk profile provided by the CEO (or the CRO or another member of the senior management team) to the board. Internal Audit reporting on the effectiveness of risk management processes is being cautiously championed by the Institute of Internal Auditors (IIA) globally through its Professional Practice Standard #2120, and through the creation of a new professional certification, Certification in Risk Management Assurance (CRMA).

**Recommendation #5: Change the mandate of ERM functions**

In many organizations, particularly financial services organizations, regulators have demanded implementation of formal ERM frameworks. Based on the analysis of codification efforts earlier in the paper, these calls for demonstrable board risk oversight are expected to significantly increase in the years ahead. Unfortunately, in a large majority of companies that have embarked on the ERM journey, they have, often with the blessing and encouragement of regulators, responded by hiring or contracting staff to create and maintain “risk registers”. These projects have often rapidly degenerated to an annual compliance exercise that results in updating risk registers to present the top 10/20/50/100 risks to the board. Few of these initiatives, in spite of significant outlays of organizational resources, are producing optimally relevant, meaningful and actionable retained risk status information for boards.

We recommend that the ERM functions be clearly tasked with assisting their organizations with implementation and maintenance of risk appetite frameworks capable of meeting the type of risk oversight expectations identified by the NACD and FSB. As noted earlier, this is unlikely to happen as long as internal audit and ERM functions continue to be “supply driven”, with ERM groups focused on creating and maintaining risk registers; internal audit functions continuing to focus on “audit universes” and providing subjective opinions on control effectiveness; and other specialist groups like external audit, safety, quality, and environment all continuing to “do their own thing”.

**Recommendation #6: Recognize misaligned reward systems present risks to good governance**

Earlier in this Directors Note we discussed root causes of the global financial crisis outlined in the 2009 SSG report. The role of compensation/reward systems, although only indirectly referenced

---


in the second SSG bullet point, not only played a key role in the global crisis but also significantly influenced the other listed root causes. It makes obvious sense that the SEC, when introducing new proxy disclosure risk oversight reporting requirements in 2009, also required U.S. public companies disclose what steps boards have taken to identify misaligned, high risk reward systems.

In spite of some progress in this area, we believe that not enough has been done to-date to truly examine the risks that misaligned reward systems represent to effective corporate governance. A recent Harvard Business Review survey of companies in Europe found that “companies have been slow to adopt risk-based incentives as part of compensation. Only 12% said they align risk management with executive pay.”

Boards need to explicitly demand that internal audit, external audit, ERM functions, safety, environment, compliance and other specialist functions pay careful attention to the potential risks posed by misaligned reward systems. Boards need to “demand” this information from assurance providers and senior management teams on a regular basis.

**Recommendation #7: Recognize the need for training**

A large percentage of boards are comprised of senior business executives with decades of experience confronting and managing all kinds of risks on a daily basis. It is only natural that a significant percentage of board efforts to date to oversee management’s risk appetite and tolerance have been similarly intuitive and lacking in formality and transparency. The new and emerging board risk oversight expectations render this largely invisible, “seat-of-the-pants/gut feel” approach to risk management untenable if the goal is to meet today’s escalating board risk governance expectations.

To bridge this gap board should “demand” a formal assessment 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 “good enough” or, stated another way, “fit for purpose”.

**Recommendation #8: Recognize and accept that better documented risk management is a “two edged sword”**

As boards and companies accelerate efforts to implement more transparent and demonstrable risk management systems it is somewhat ironic that they will, almost certainly, elevate their litigation and regulatory risk levels unless careful steps are taken to manage, or in risk speak, “treat” the potential risks that come with increased levels of documented knowledge of management and the board’s risk appetite and tolerance.

---

Although not much has been written to analyze the state of law in countries around the world in this area, the following excerpt written with compliance programs in mind also applies to risk management and risk oversight:

Of course, compliance audits are a two edged-sword. Demonstration that a systematic compliance audit has been carried out by competent personnel should be strong evidence of reasonable care. Production of such an audit in evidence by the defendant would necessitate the prosecutor adducing substantial expert evidence to displace the inference of due diligence that it would suggest, unless it was apparent, on its face or in light of other evidence, that the audit was perfunctory or that the accused should have recognized its inadequacy. On the other hand, such an audit not only describes and diagnoses, but also prescribes. For this reason, an audit showing that an actual or potential non-compliance had been discovered and recommending remedial steps that were not carried out would be cogent evidence of lack of reasonable care. This has resulted in reluctance to carry out such program, attempts to design them so they are privileged, and lobbying for legislation or policies that would prevent their use as evidence against the accused in prosecutions.” 30

There are numerous examples in the business press that suggest companies, through decisions of their senior management and, in some cases the board of directors, consciously accepted illegality, breach of contract, manipulation of LIBOR rates, money laundering, bribery of foreign officials, dangerously defective and unsafe products and services, pollution of the environment, sexual harassment and discrimination, fraudulently misleading financial disclosures, investments with high potential to implode, and other acts of omission and commission. Unfortunately, or fortunately depending on your perspectives, better and more formal risk management processes have the potential to “burden” boards with the documented knowledge of these risk tolerance decisions. It would be naïve to assume that all boards will equally welcome the burden of being legally aware of and accepting of this type of risk acceptance. While there are specific strategies that can be employed by all involved in risk governance to manage litigation risk, few risk specialists have received much training on how to spot and deal with “risky” risk status/profile disclosures.

Board Risk Oversight of Management’s Risk Appetite and Tolerance: Utopian Fantasy or Stretch Objective?

This Director Note has overviewed the rapidly emerging codification of board risk oversight expectations and chronicled a list of significant handicaps boards face meeting these new expectations. Eight recommendations to address serious handicaps posed by status quo approaches to risk management and assurance in wide spread use around the world are proposed. The recommendations are transformational in spirit and scope. We recognize however, that the human tendency is to prefer incremental over transformational change. Unfortunately, the preference for an incremental approach to change often results in progress that is, as the age old adage goes, “too little, too late”. On a positive note, there are many companies and boards capable of embracing

---

these new expectations as an opportunity to increase stakeholder value and trust, not solely an exercise to appease regulatory demands. It will be the boards and the organizations and stakeholders they serve that see better board oversight of management’s risk appetite and tolerance as a stretch objective, not a utopian fantasy that will set the new board risk oversight standards in the years ahead.
Sample Board/Demand 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 all stakeholders, internal and external. Benefits foreseen are:

- Increase the likelihood of achieving the company’s business objectives.
- Enhance XYZ’s competitive advantage.
- Deal with market instability more effectively.
- Enable XYZ to better meet customers’ expectations and contractual requirements.
- Establish a Board level mandate to implement an enterprise wide approach to risk management to meet emerging risk management and risk oversight expectations.
- Enhance shareholder and customer confidence.
- Respond to escalating institutional shareholder demands for effective risk management frameworks in companies they invest in.
- Meet emerging 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 the helps decision makers and
the board better understand the level of uncertainty that exists that business objectives will 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 that there are reliable processes in place to provide the board of directors with an annual report on the effectiveness of the Corporation’s risk management processes, and periodic reports on the Corporation’s consolidated residual risk status, including any 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 business 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 risks and external risks that have the potential to impact on the business unit’s key objectives together with their 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 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 Information Form (AIF) related to risk management and oversight.
Attachment 2

RiskStatusline™

End Result Objective
(Implicit or Explicit)

External and Internal Environment
the organisation seeks to achieve its objectives.

Internal/External Context

Threats to Achievement/Risks?

External and Internal Environment
the organisation seeks to achieve its objectives.

Threats to Achievement/Risks are real or possible situations that create uncertainty regarding achievement of the objective.

Risk Treatment Strategy
risk mitigators/controls
risk transfer, share, finance
(Selected consciously or unconsciously)

Risk Treatments manage uncertainty that the objective will be achieved by mitigating, transferring, financing, or sharing risks.

Residual Risk Status

Residual Risk Status is a composite snapshot that helps decision makers assess the acceptability of the retained risk position.

Status data includes performance data, potential impact(s) of not achieving the objective, impediments, and any concerns regarding risk treatments in place. (NOTE: “control deficiencies” are called concerns)

Acceptable?

Is the residual risk status acceptable to the work unit? Management? The Board? Other key stakeholders? (i.e. managed within risk appetite/tolerance)

NO
Re-examine risk treatment strategy and/or objective and develop action plan

YES – Move On

YES

Risk Treatment Optimized?

Is this the lowest cost combination of risk treatments given our risk appetite/tolerance?

NO

© 2012 Risk Oversight Inc.