Board Driven/Objective Centric ERM & Internal Audit: Next Generation Assurance

Tim Leech, FCPA, CIA, CRMA, CCSA, CFE
Managing Director Global Services
Risk Oversight Inc.

October 2013
Your Presenter

Tim Leech
Managing Director Global Services
Risk Oversight Inc.
www.riskoversight.ca
tim.leech@riskoversight.ca
www.twitter.com/riskoversight
About Your Presenter

Tim J. Leech, FCPA FCA CIA CRMA CCSA CFE is Managing Director Global Services at Risk Oversight Inc. (“RO”) He has over 30 years of experience in the ERM, internal audit, IT, and forensic/litigation accounting fields. His experience base includes setting up a new business unit for Coopers & Lybrand (Control & Risk Management Services) in 1987; founding, building, and successfully selling CARD®decisions, a global risk and assurance consulting and software firm, to Paisley/Thomson Reuters from 1991 to 2004; serving as Paisley’s Chief Methodology Officer from 2004 -2007; and global experience helping clients with internal audit transformation initiatives and the design, implementation, and maintenance of integrated GRC/ERM methodology and technology frameworks. He developed and successfully released CARD®map, the world’s first integrated risk and assurance software, in 1997. The web-enabled “cloud” version of CARD®map was released in 2000. He has delivered IIA IPPF Standard 2120 training on how to assess and report on the effectiveness of risk management processes to internal auditors and risk specialists in locations around the world. He is the author of the December 2012 Conference Board Director Notes publication “Board Oversight of Management’s Risk Appetite and Tolerance” and the globally acknowledged RO white paper “The High Cost of ERM Herd Mentality”. Risk Oversight Inc. and BPS Resolver will be launching RiskStatusNet™ - “next generation” ERM/GRC software in late 2013. In 1997 Leech was awarded the designation Fellow of the Ontario Institute of Chartered Accountants (FCPA/FCA) in recognition of his public service and contributions in the fields of risk and control management. In September 2009 Tim was awarded the first ever IIA Canada Outstanding Contributor to the Profession of Internal Auditing award in recognition of over 25 years of global service to the internal audit profession.
Agenda

• Board Risk Oversight: Utopian Fantasy or Stretch Objective?
• Positive Fallout from 2008 Global Financial Crisis: Better Board Risk Oversight
• Codification of board risk oversight expectations
• Handicaps boards face meeting the new expectations
• Recommendations
• New Tools Required
• Questions
Board Risk Oversight: Utopian Fantasy or Stretch Objective?

An impractical, idealistic scheme for social and political reform

http://www.thefreedictionary.com/utopia

Definition

That cannot be achieved by incremental or small improvements but require extending oneself to the limit to be actualized. Expressed in the saying, "You cannot cross a chasm in two steps."
Positive Fallout from 2008 Global Financial Crisis: Better Board Risk Oversight

Bear Stearns bailout

J.P. Morgan and N.Y. Fed provide funds to strapped Wall St. broker

Extraordinary action taken after Bear Stearns by CEO's admission, suffers a significant 24-hour relaxation from its liquidity position. J.P. Morgan statement suggests an endgame is yet to play out.

Bear Stearns' troubles (First Take)

A gristy day for Bear and peers

Bear Stearns bailout

MARKET SNAPSHOT: STREET REACTS TO BAILOUT

- Markets
  - Bailout news alerts U.S. stocks
  - Moves & Shakes for Friday
  - Morgan, Bear Stearns
  - Fed funds futures point to higher likelihood of a 50-point rate cut

So long, Bear Stearns BSC

Final bid, $2

Lehman collapse sends shockwave round world

AIG Faces $17B in Collateral Calls

Under New Management - You Just Bought It!

2013 All Star Conference
October 14-16, 2013 / New Orleans, LA, USA

The Institute of Internal Auditors
Codification of Board Risk Oversight Expectations
Codification of Board Risk Oversight Expectations

Senior Supervisors Group issued three important reports:


3. December 23, 2010 “Observations on Developments in Risk Appetite Frameworks and IT Infrastructure”

Codification of Board Risk Oversight Expectations

- 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.

Codification of Board Risk Oversight Expectations

REPORT OF THE NACD BLUE RIBBON COMMISSION

RISK GOVERNANCE: BALANCING RISK AND REWARD

PUBLISHED BY National Association of Corporate Directors
SPONSORED BY The Center for Board Leadership
AND ITS ALLIANCE PARTNERS Heidrick & Struggles International, Inc.
Codification of Board Risk Oversight Expectations

NACD Board Risk Oversight Criteria

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.

• management has implemented a system to manage, monitor, and mitigate risk, and that system is appropriate given the company’s business model and strategy.
Codification of Board Risk Oversight Expectations

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

- 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.

Codification of Board Risk Oversight Expectations

A FRAMEWORK FOR BOARD OVERSIGHT OF ENTERPRISE RISK

by John E. Caldwell, CA
Codification of Board Risk Oversight Expectations

CSA Expectations: Canadian Public Companies

Material risks are required to be disclosed in regulatory filings such as an AIF or a prospectus. The way in which an issuer manages those risks may vary between industries and even between issuers within an industry according to their particular circumstances. It is important for investors to understand how issuers manage those risks.

Disclosure regarding oversight and management of risks should indicate:

- the board’s responsibility for oversight and management of risks, and
- any board and management-level committee to which responsibility for oversight and management of risks has been delegated.

The disclosure should provide insight into:

- the development and periodic review of the issuer’s risk profile
- the integration of risk oversight and management into the issuer’s strategic plan
- the identification of significant elements of risk management, including policies and procedures to manage risk, and
- the board’s assessment of the effectiveness of risk management policies and procedures, where applicable.

ICGN Corporate Risk Oversight Guidelines
SECURITIES AND EXCHANGE COMMISSION

17 CFR PARTS 229, 239, 240, 249 and 274

[RELEASE NOS. 33-9089; 34-61175; IC-29092; File No. S7-13-09]

RIN 3235-AK28

PROXY DISCLOSURE ENHANCEMENTS

AGENCY: Securities and Exchange Commission.

ACTION: Final rule.

SUMMARY: We are adopting amendments to our rules that will enhance information provided in connection with proxy solicitations and in other reports filed with the Commission. The amendments will require registrants to make new or revised disclosures about: compensation policies and practices that present material risks to the company; stock and option awards of executives and directors; director and nominee qualifications and legal proceedings; board leadership structure; the board’s role in risk oversight; and potential conflicts of interest of compensation consultants that advise companies and their boards of directors. The amendments
Codification of Board Risk Oversight Expectations

FROM THE SEC February 20, 2013:

Item 407(h) also requires companies to describe the role of the board of directors in the oversight of risk. Recently, the U.S. Government Accountability Office found that economic output losses from the 2007-2009 financial crisis could exceed $13 trillion. Given the magnitude of that crisis, which continues to be felt, it would be difficult to overemphasize the importance that investors place on questions of risk management. Has the board set limits on the amounts and types of risk that the company may incur? How often does the board review the company’s risk management policies? Do risk managers have direct access to the board? What specific skills or experience in managing risk do board members have? Issuers that offer boilerplate in lieu of a thoughtful analysis of questions such as these have not fully complied with our proxy rules and are missing an important opportunity to engage with investors.

Source: SEC Commissioner Speech Louis Aguilar, February 20, 2013
Codification of Board Risk Oversight Expectations

Thematic Review on Risk Governance

Peer Review Report

Table of Contents

Foreword .............................................................. i
Glossary ................................................................... ii
Executive summary .................................................. 1

I. Introduction ....................................................... 6

II. National authorities’ oversight of risk governance practices .................................. 8
   1. The board and its committees ........................................... 9
      1.1 Board composition ........................................... 9
      1.2 Governance of the board .................................. 11
   2. The firm-wide risk management function ......................... 11
      2.1 Governance of the risk management function ........ 11
      2.2 Risk appetite framework ............................... 12
      2.3 Stress testing ............................................. 13
   3. Independent assessment of firms’ risk governance framework ................... 14
      3.1 Internal audit ............................................. 14
Codification of Board Risk Oversight Expectations

Recommendations:

1. To ensure that firms’ risk governance practices continue to improve, FSB member jurisdictions should strengthen their regulatory and supervisory guidance for financial institutions, in particular for SIFIs, and devote adequate resources (both in skills and quantity) to assess the effectiveness of risk governance frameworks. In particular, national authorities should consider the following sound risk governance practices:

   i. set requirements on the independence and composition of boards, including requirements on relevant types of skills that the board, collectively, should have (e.g., risk management, financial industry expertise) as well as the time commitment expected.

   ii. hold the board 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. This includes establishing communication procedures between the risk committee and the board and across other board committees, most importantly the audit and finance committees.

   iii. set requirements to elevate the CRO’s stature, authority, and independence in the firm. This includes requiring the risk committee to review the performance and objectives of the CRO, ensuring the CRO has unfettered access to the board and risk committee (including a direct reporting line to the board and/or risk committee), and expecting the CRO to meet periodically with directors without executive directors and management present. The CRO should have a direct reporting line to the CEO and a distinct role from other executive functions and business line responsibilities (e.g., no “dual-hatting”). Further, the CRO should be involved in activities and decisions (from a risk perspective) that may affect the firm’s prospective risk profile (e.g., strategic business plans, new products, mergers and acquisitions, internal capital adequacy assessment process, or ICAAP).

   iv. require the board (or audit committee) to obtain an independent assessment of the design and effectiveness of the risk governance framework on an annual basis.
Codification of Board Risk Oversight Expectations

Principles for An Effective Risk Appetite Framework

Consultative Document

17 July 2013
Codification of Board Risk Oversight Expectations

4.1 The board of directors should:

a) approve the firm’s RAF, 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;
Board Risk Oversight Handicaps
“Asymmetric Information”
Board Risk Oversight Handicap #2

Lack of consensus what it means
Board Risk Oversight Handicap #3

Traditional IA/ERM not delivering what boards need
Board Risk Oversight Handicap #4

Traditional “Supply Driven” Assurance

Approach #2: Internal and external auditors form/report subjective opinions on whether they think controls are “effective” or “adequate”

Question: If the objective is “Prevent/minimize injuries/deaths in the home due to fire”, how many “controls” must be present to conclude controls are “effective” or “adequate”?

Should there be a tested escape plan? Should there be a fire extinguisher in the kitchen? In other rooms? Should there be two kinds of smoke detectors, battery and wired? Should there be a fire blanket in the kitchen? Should the house have a sprinkler system? Should parents have burn prevention/treatment training? Should there be an annual inspection by the local fire department or a fire risk specialist? Should there be an annual documented risk assessment that cover statistically probable risks? What about insurance coverage, contractual indemnities with suppliers, etc?

Answer: There is no such thing in real life as “effective controls”, only different levels of acceptable retained/residual risk. Auditors and regulators continue to pretend this isn’t a fundamental truth.

Subjective opinions on control “effectiveness” from Internal Audit
Board Risk Oversight Handicap #5

Credit agencies & boards unsure what’s required

PRESS RELEASE
Nov. 14, 2012, 3:00 p.m. EST

NACD Convenes Inaugural Advisory Council on Risk Oversight
Fortune 500 Committee Chairs and Corporate Governance Leaders Meet to Discuss Board Risk Oversight

WASHINGTON, Nov 14, 2012 (GlobeNewswire via COMTEX) -- The National Association of Corporate Directors (NACD) convened its inaugural Advisory Council on Risk Oversight Oct. 28th to discuss the current environment in risk oversight for corporate boards. NACD was supported by partners PwC and Gibson, Dunn & Crutcher LLP.

Amid Hurricane Sandy, members of the delegation met telephonically to discuss the current and emerging risks facing directors. In the abbreviated meeting, the council discussed two important issues: allocation of risk and the new era of reputational risk oversight.

"Assembling directors and key stakeholders is crucial to understanding each party's expectations and making a more informed decision about how to achieve better oversight," said Ken Daly, president and CEO of NACD. "Through advisory councils like this, we can..."
Board Risk Oversight Handicap #6

Two-edged sword: “Damned if we do/Damned if we don’t”
Board Risk Oversight Handicap #7

Boards simply haven’t asked for the information they need
Recommendations
Transition IA & ERM from “supply driven” to “board/demand driven”
Clarify accountabilities of all parties
Focus on end result objectives

Risk Assessment on: “I want to be somewhere west of here” versus “I want to be at 123 Street, Oakville, Ontario by Friday at 10.00 EST”
Change IA’s mandate

2120 – Risk Management

The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

*Interpretation:*
Determining whether risk management processes are effective is a judgment resulting from the internal auditor’s assessment that:

- Organizational objectives support and align with the organization’s mission;
- Significant risks are identified and assessed;
- Appropriate risk responses are selected that align risks with the organization’s risk appetite; and
- Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.

The internal audit activity may gather the information to support this assessment during multiple engagements. The results of these engagements, when viewed together, provide an understanding of the organization’s risk management processes and their effectiveness.

Issued: October 2008
Revised: October 2012
Change mandate of ERM functions

Recommendations:

1. To ensure that firms’ risk governance practices continue to improve, FSB member jurisdictions should strengthen their regulatory and supervisory guidance for financial institutions, in particular for SIFIs, and devote adequate resources (both in skills and quantity) to assess the effectiveness of risk governance frameworks. In particular, national authorities should consider the following sound risk governance practices:

   i. set requirements on the independence and composition of boards, including requirements on relevant types of skills that the board, collectively, should have (e.g., risk management, financial industry expertise) as well as the time commitment expected.

   ii. hold the board 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. This includes establishing communication procedures between the risk committee and the board and across other board committees, most importantly the audit and finance committees.
Recognize reward system risk
Recognize need for training
Recognize dangers of the two-edged sword

“Damned if we do”
“Damned if we don’t”
New Tools Required
NEW TOOLS REQUIRED

ABC CORP OBJECTIVES REGISTER

As at June 18, 2013
## NEW TOOLS REQUIRED

### ABC CORP

**REVENUE/PROFIT MAXIMIZATION/VALUE CREATION**

<table>
<thead>
<tr>
<th>Draft objective statement</th>
<th>Objective Source</th>
<th>Owner/Sponsor Candidate</th>
<th>CRRR</th>
<th>CRRR Update Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimise losses as a result of FX fluctuations on fee income</td>
<td>Risk Register #63</td>
<td></td>
<td>N/R</td>
<td></td>
</tr>
<tr>
<td>Deliver returns of 5% p.a. net outperformance over public markets over a 10 year period</td>
<td>2012 Interim Report p1</td>
<td></td>
<td>N/R</td>
<td></td>
</tr>
<tr>
<td>Deliver a level of annual returns reflecting the returns that top quartile private equity funds will generate in the long term</td>
<td>2012 Interim Report p2</td>
<td></td>
<td>N/R</td>
<td></td>
</tr>
<tr>
<td>Increase the frequency of positive media coverage</td>
<td>Risk Register</td>
<td></td>
<td>N/R</td>
<td></td>
</tr>
<tr>
<td>Develop funding alternatives to the Revolving Credit Facility (“RCF”)</td>
<td>Board presentation</td>
<td></td>
<td>N/R</td>
<td></td>
</tr>
<tr>
<td>Expand ABC’s RCF</td>
<td>Board presentation</td>
<td></td>
<td>N/R</td>
<td></td>
</tr>
</tbody>
</table>
## NEW TOOLS REQUIRED

<table>
<thead>
<tr>
<th>Draft objective statement</th>
<th>Objective Source</th>
<th>Owner/Sponsor Candidate</th>
<th>CRRR</th>
<th>CRRR Update Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure the company complies with UK Listing Authority’s Listing Rules</td>
<td>2011 Annual Report page 100</td>
<td></td>
<td>N/R</td>
<td></td>
</tr>
<tr>
<td>Ensure that the company complies with the disclosure rules established by the FSA</td>
<td>Risk Register</td>
<td></td>
<td>N/R</td>
<td></td>
</tr>
<tr>
<td>Ensure compliance with the UK Bribery Act 2010</td>
<td>Compliance view of the highest potential value erosion laws/regulations</td>
<td></td>
<td>N/R</td>
<td></td>
</tr>
<tr>
<td>Ensure all staff meet or exceed applicable civil standards of fiduciary duty in the roles they play</td>
<td>Risk Register/Discussion with Stuart Ballard</td>
<td></td>
<td>N/R</td>
<td></td>
</tr>
<tr>
<td>Ensure compliance with all applicable employment law rules and regulations</td>
<td>Risk Register</td>
<td></td>
<td>N/R</td>
<td></td>
</tr>
<tr>
<td>Ensure all applicable laws and regulations related to offshore funds are complied with</td>
<td>Risk Register</td>
<td></td>
<td>N/R</td>
<td></td>
</tr>
<tr>
<td>Ensure compliance with all applicable Dodd Frank Rules</td>
<td>Risk Register #335</td>
<td></td>
<td>N/R</td>
<td></td>
</tr>
<tr>
<td>Ensure the company complies with the UK Governance Code</td>
<td>Risk Register #272</td>
<td></td>
<td>N/R</td>
<td></td>
</tr>
<tr>
<td>Ensure the company complies with all applicable laws and regulations related to employee health/safety</td>
<td>Risk Register #42</td>
<td></td>
<td>N/R</td>
<td></td>
</tr>
</tbody>
</table>
NEW TOOLS REQUIRED
NEW TOOLS REQUIRED

**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 of 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.
# New Tools Required

<table>
<thead>
<tr>
<th>Risk Status Analysis Level</th>
<th>Overview of Assessment Options</th>
</tr>
</thead>
</table>
| **Quick Start**           | • Define/refine end result business objectives and “Owner/Sponsors”  
                           | • Assign an initial Residual Risk Status rating for each objective from 0 (fully acceptable) to 10 (entity catastrophic). The rating is linked to the level of management/board attention. |
| **Importance Prioritization Option** | • Quick Start requirements (see above)  
                           | • Assign an objective importance rating – importance to the unit  
                           | • Assign an objective importance rating – importance to the entire corporation  
                           | • Document current level of risk status knowledge and target level. The higher the gap between current and target the higher the objective’s priority. |
| **High Level Risk Assessment** | • Quick Start and Importance Prioritization options (see above)  
                           | • Document threats to achievement/risks, likelihood and consequences of risks, and risk level  
                           | • Document “best guess” current mitigation estimate for each threat/risk and traffic light rating  
                           | • Develop and assign responsibility for risk treatment action items for risks with unacceptable residual risk ratings |
| **Full RiskStatusline™ Assessment** | All steps above plus:  
                           | • Document key risk treatments in place to manage significant risks  
                           | • Document current performance information for the objective using best available information (“KPI” information)  
                           | • Document impact information for the objective including what would be the consequences to company, unit, individuals, community etc if the objective wasn’t achieved in whole or part. (NOTE: This is impact of non-achievement of objective not individual risks impacts)  
                           | • Document known concerns – risk treatments/controls known to be missing, deficient or needing improvement  
                           | • Document any impediments - elements outside of the control/resources of the business objective owner that would prevent them from adjusting retained risk level  
                           | • Assign action items |
NEW TOOLS REQUIRED
Consolidated Report On Risk

Very simply, consolidated residual risk reports provide details on important value creation and potential value erosion objectives that have high residual risk ratings (see prior slides). High RRRs indicate increasingly material unacceptable retained risk positions with potential to have a significant negative impact on the achievement of specified end result objectives.
NEW TOOLS REQUIRED
Technology capable of producing real time reports on risk status

RiskStatusNet™ Goals:
• Better Meet Board Risk Oversight Expectations
• Better Integration of Assurance Efforts
• ERM Transformation
• Optimize Risk Treatments
• Transparent Scope
• Internal Audit Reports Provide Risk Management Training
• Transparent Assurance
• Risk Management Rigor Fit for Purpose
• Transition from “Direct Report” to “Attestation Auditing”
• Transition from “Controls” to “Risk Treatments”
Questions???

Tim Leech
tim.leech@riskoversight.ca
www.riskoversight.ca

Twitter: www.twitter.com/riskoversight