Audit Transformation Strategies to Meet Escalating Stakeholder Expectations

Module 1: Escalating Stakeholder Expectations & The Way Forward

Tim Leech, Managing Director
Risk Oversight Solutions Inc.
timleech@riskoversightsolutions.com

www.riskoversightsolutions.com

Mountains of Change...Oceans of Opportunities
Workshop Agenda

Speaker Background & Introduction

Module 1: Escalating Expectations

- Session Objectives
- Escalating Expectations: Regulators
- Escalating Expectations: Credit Agencies
- Escalating Expectations: Institutional Investors
- Escalating Expectations: Public Sector
- Escalating Expectations: Director Associations
- Escalating Expectations: Internal Audit Customers
- Group Discussion: Barriers to Meeting New Expectations
- IIA Response & The Way Forward
Module 2 Board & C-Suite Driven/Objective Centric ("BCD/OC") ERM and IA

- BCD/OC Design Objectives
- BCD/OC Core Elements
- BCD/OC Key Benefits to IA
- BCD/OC Examples
- BCD/OC Tools
- Group Discussion: Barriers to Implementing BCD/OC
- BCD/OC Implementation Barriers
- BCD/OC Implementation Steps & Options
Workshop Objectives

- Overview escalating IA stakeholder expectations
- Analyze causes of growing IA customer dissatisfaction
- Provide a forum to discuss barriers to meeting the new stakeholder expectations
- Overview steps taken by IIA Global to date
- Overview core elements of Board & C-Suite Driven/Objective Centric (BCD/OC) – a new approach to ERM and Internal Audit
- Provide a forum to discuss barriers to implementing BCD/OC
- Overview some BCD/OC implementation options
Escalating Expectations: Regulators

Financial Reporting Council

Canadian Securities Administrators
Autorités canadiennes en valeurs mobilière

Financial Stability Board
Escalating Expectations: Regulators

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.

Source: CSA STAFF NOTICE 58-306 2010 CORPORATE GOVERNANCE DISCLOSURE COMPLIANCE REVIEW
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.
4.1 The board of directors should:

a) approve the financial institution’s RAF, developed in collaboration with the CEO, CRO and CFO, and ensure it remains consistent with the institution’s short-and-long-term strategy, business and capital plans, risk category 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 the 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 the actual risk profile and risk limits against the agreed levels (e.g. by business line, legal entity, product, risk category), including qualitative measures of conduct risk;

f) discuss and monitor to ensure appropriate action is taken 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.
Escalating Expectations: Regulators

Financial Stability Board (“FSB”) November 2013:

4.6 **Internal audit (or other independent assessor) should**:

a) routinely include assessments of the RAF on an institution-wide basis as well as on an individual business line and legal entity basis;

b) identify whether breaches in risk limits are being appropriately identified, escalated and reported, and report on the implementation of the RAF to the board and senior management as appropriate;

c) independently assess periodically the design and effectiveness of the RAF and its alignment with supervisory expectations;

d) assess the effectiveness of the implementation of the RAF, including linkage to organisational culture, well as strategic and business planning, compensation, and decision-making processes;

e) assess the design and effectiveness of risk management techniques and MIS used to monitor the institution’s risk profile in relation to its risk appetite;

f) report any material deficiencies in the RAF and on alignment (or otherwise) of risk appetite and risk profile with risk culture to the board and senior management in a timely manner; and

g) evaluate the need to supplement its own independent assessment with expertise from third parties to provide a comprehensive independent view of the effectiveness of the RAF.
Boards are responsible for:

- determining the extent to which the company is willing to take on risk (its “risk appetite”);
- ensuring that an appropriate “risk culture” has been instilled throughout the organization;
- identifying and evaluating the principal risks to the company’s business model and the achievement of its strategic objectives, including risks that could threaten its solvency or liquidity;
- agreeing how these risks should be controlled, managed, or mitigated;
Boards are responsible for (continued):

- ensuring an appropriate risk management and internal control system is in place, including a reward system;
- reviewing the risk management and internal control systems and satisfying itself that they are functioning effectively and that corrective action is being taken where necessary; and
- taking responsibility for external communication on risk management and internal control.

Escalating Expectations: Credit Agencies

Global Credit Portal
RatingsDirect

June 14, 2006

Credit FAQ:
Standard & Poor's Looks Further Into How Nonfinancial Companies Manage Risk

Primary Credit Analyst:
Sharon J. Doogy, New York (212) 521-7893, doogy_sharon@standardpoors.com

Table Of Contents
Frequently Asked Questions

www.standardandpoors.com/ratingsdirect

Special Comment

August 2006

Best Practices for a Board's Role in Risk Oversight

Summary
Moody's views a board of directors' role overstepping a critical role in the running of an enterprise — especially for financial institutions and for other companies with significant market and credit risk exposure. In particular, Moody's sees high expectations for board's role in shaping firm's risk appetite and securing a proper risk-management framework is place. (By board, Moody's typically refers to the board of directors. In those jurisdictions with a dual board structure, we refer to the risk of the supervisory board.)

In Moody's view, the board has several functions with respect to risk:
1. Approve the firm's risk appetite as a component of its strategy
2. Understand and question the board of risk faced by the company
3. Ensure the oversight of risk is the board's management oversight and senior management level
4. Promote a risk-focused culture and open communication across the organization
5. Assign clear lines of accountability and encourage an effective risk management framework

The special comment describes how Moody's views best practices for the role of boards of directors in risk oversight. Moody's evaluates these practices so that investors can identify those best practices and determine whether the company's risk oversight is adequate. Moody's will emphasize the importance of our analysis in this context.

Moody's Investors Service
Global Credit Research

Moody's Investors Service
Global Credit Research
S&P: “We believe that successful risk culture begins with fostering open dialogue where every employee in the organization has some level of ownership of the organization's risks, can readily identify the broader impacts of local decisions, and is rewarded for identifying outsize risks to senior levels. In such cultures, strategic decision-making routinely includes a review of relevant risks and alternative strategies rather than a simple return-on-investment analysis.” (page 4)
Escalating Expectations: Institutional Investors

Corporate Risk Oversight Committee

The committee seeks to influence policies relating to corporate risk oversight. This includes (1) guidelines on what constitutes best practice in corporate risk oversight; and (2) the responsibilities of shareholders and companies with respect to corporate risk oversight and how this is communicated.

Committee Members (2014 - 2015)

Carola van Lamoen, Co-chair, Robeco, Netherlands

Brian Barner, Co-chair, ValueBridge Advisors, USA
Escalating Expectations: Institutional Investors

ICGN Corporate Risk Oversight Guidelines
Escalating Expectations: Public Sector

Treasury Board of Canada Secretariat

Framework for the Management of Risk

1. Effective Date
2. Context
3. Linkages to Other Treasury Board Instruments
4. Purpose
5. Principles
6. Roles and Responsibilities
“The Secretariat also monitors and assesses departmental and agency performance on risk management through such means as the Management Accountability Framework, and reviews of internal and external audits. These assessments may be used to inform discussions between the Secretary of the Treasury Board and Deputy Heads.

Evidence that a federal department or agency has effective risk management practices in place may lead to Treasury Board and Secretariat oversight being adjusted to an organization's capacity for managing risk, where circumstances permit. Conversely, ineffective risk management may lead to additional controls and oversight. Where necessary, the Secretariat may encourage deputy heads to undertake appropriate remedial measures in support of their responsibilities for the monitoring of risk management within their organization.”

Escalating Expectations: Director Associations
Escalating Expectations: IA Customers
Escalating Expectations: IA Customers

Figure 4. Satisfaction with internal audit value and performance

- Percent of stakeholders reporting internal audit provides “significant value”
  - 2013: 79% (Board Members), 68% (Senior Management)
  - 2014: 64% (Board Members), 49% (Senior Management), 65% (CAEs)

- Percent of 2014 respondents reporting that internal audit “performs well”
  - 2013: 64% (Board Members), 45% (Senior Management)
  - 2014: 65% (CAEs)

Internal audit may need a makeover

By Ken Tysiac
March 16, 2015

Many internal audit functions will need to undergo a fundamental shift in the coming years to keep pace with changes at their organizations, according to a new survey report.

Just 11% of chief audit executives (CAEs) participating in PwC’s 2015 State of the Internal Audit Profession Study say their current internal audit function is providing value-added services and proactive advice for the business. But 60% of CAEs believe they need to be providing such services and advice within the next five years.

Meanwhile, more than 45% of internal audit stakeholders expect internal audit to move from its traditional role of providing assurance to a more proactive advisory role within the next five years.

In many cases, internal audit will be undergoing a makeover along with the rest of the business. Nearly 70% of organizations participating in the survey have gone through or are in the process of a business transformation in response to market shifts. An additional 12% plan such a transformation in the next 18 to 24 months.
Most Internal Auditors See Role Becoming More Strategic

But only 11% of chief audit executives see their current internal audit function as providing value-added services and proactive advice.

Matthew Heller

March 16, 2015 | CFO.com | US

Amid a rapidly changing business landscape, most internal auditors see themselves moving beyond their traditional assurance provider role and becoming proactive advisers to corporations, according to PricewaterhouseCoopers.

PwC’s latest State of the Internal Audit Profession survey found that while only 11% of chief audit executives see their current internal audit function as providing value-added services and proactive advice, 60% of CAEs and just over 45% of stakeholders expect the function to have a more proactive role within the next five years.

The report also identifies four key areas that will enable internal audit to contribute to organizations’ strategic and transformational initiatives, including risk, focus, talent...
Similarly, PwC survey results – which reflect the opinions of more than 1,900 CAEs, internal audit managers, senior management, and board members – indicate significant dissatisfaction with internal audit value and performance. Taking into account the respondents who did not know whether internal auditing adds significant value to the organization, the survey results show that 50 percent of senior management and 28 percent of board members believe internal auditing adds less than significant value to their organization. Furthermore, only 49 percent of senior management and 64 percent of board members believe internal auditing is performing well at delivering on expectation (Figure 4). Also noteworthy, the belief among board members that internal audit adds significant value has dropped 10 points from last year. Evident from these findings, an expectation gap exists between stakeholders and the internal audit activity.
Figure 5. Distinctions between the lines of defense

Regarding the clarity between your organization's various “lines of defense,” how clear are the distinctions between the roles of internal audit and your organization’s management, risk, compliance, and control functions?

- Very Clearly Defined, 36%
- Moderately Defined, 32%
- Somewhat Defined, 21%
- Not Clearly Defined, 11%

64%

Source: The IIA’s Audit Executive Center Global Pulse of the Profession survey, 2014. This chart reflects data from the global CAE respondents of the survey.
Escalating Expectations: IA Customers

Figure 6. In the year ahead, in which of the following areas would you like your internal audit function to devote more of its time and/or sharpen its focus? (Select all that apply.)

- Risk Management Processes: 65%
- Information Technology and Data Management: 58%
- Operational Risks: 52%
- Compliance and Regulation: 45%
- Corruption/Fraud: 36%
- Ethics and Culture: 28%
- Corporate Governance: 27%
- Cost Reduction/Enhancement: 25%
- Change Management: 21%
- Crisis Management: 18%
- Tax Compliance: 14%
- Other: 3%
- Company Does Not Have an Internal Audit Function: 1%

Source: KPMG International's Global Audit Committee Survey, 2014. This client reflects data from only those respondents who indicated the internal audit’s role and responsibilities should extend beyond the adequacy of financial reporting and controls.
Fewer than half (49 percent) of senior management responding in PwC’s survey believe that internal audit is performing well at obtaining, training, and/or sourcing the right level of talent and the right specialists for its needs. The PwC report surmises, “As the right talent model is imperative to delivering on expectations, it is no wonder that there is such a correlation between stakeholders’ views about skillset development and their views about internal auditing’s overall performance.” There are several ways to close this gap – cosourcing, recruiting, and training. The key is to identify the gap and close it.
Group Discussion

• What barriers do you see that impede Internal Audit’s ability to meet the new stakeholder expectations described in this module?
IIA Response to Date

2120 – Risk Management

“The internal audit activity must evaluate the effectiveness and contribute to the improvement of the risk management process”
Certification in Risk Management Assurance (CRMA)

**Be a Key Advisor to the Audit Committee and Executive Management for Risk Management**

Job analysis and stakeholder surveys have indicated a key element to unlocking internal audit’s full potential can be found in a professional’s ability to provide advice and assurance on risk management to audit committees and executive management. In response, The IIA developed the CRMA designation.

The standard CRMA Core Exam will be a 100-question, multiple-choice exam, with a seat time of two hours. These exams will be instantly scored like all of the other IIA exams, and will be administered at Pearson VUE testing centers around the world. All Certification in Risk Management Assurance® (CRMA®) eligibility requirements will apply.

**The CRMA: Your Key to Career Success**

The CRMA is designed for internal auditors and risk management professionals with responsibility for and experience in providing risk assurance, governance processes, quality assurance, or control self-assessment (CSA). It demonstrates an individual’s ability to evaluate the dynamic components that comprise an organization’s governance and enterprise risk management program and provide advice and assurance around these issues.
Imagine the Possibilities!

The IIA's new chairman of the board, Paul Sobel, says internal auditors need to envision new ways to add value to their organization, and the profession as a whole.

Half a century ago, the land underlying the municipalities of Lake Buena Vista and Bay Lake, Fla. was a largely unpopulated patchwork of cattle ranches, citrus groves, scrub forests, and alligator- and snake-infested swamps. But that's not what the late Walt Disney saw in his mind's eye when he overflow those 47 square miles, just south of Orlando, in November 1953. Instead, Disney saw a prime location for a family vacation mecca.

Disney died before he could savor the first fruits of his fertile imagination, the 1971 opening of the Magic Kingdom theme park. But his vision still is very much alive. The Walt Disney World Resort's theme parks, golf courses, hotels, restaurants, retail stores, and other attractions now bring joy to nearly 30 million visitors each year.
Reinventing Internal Audit: Audit Transformation Strategies to Meet New Expectations

Course Description

Surveys conducted by The IIA, PwC, KPMG, Protiviti, and others in the first six months of 2014 indicate growing customer dissatisfaction with traditional internal audit methods and service. The July 2014 Global IIA update “The Pulse of the Profession: Enhancing Value through Collaboration: A Call to Action” calls on the profession to make radical and rapid changes to the way internal audit services and assurance is delivered.

At the July International Conference in London and through articles, blogs and other presentations, IIA leaders are stressing to IIA members around the world the need for urgent and significant changes.

The new emerging customer expectations linked to significantly heightened risk oversight expectations have profound implications for internal auditors, ERM teams, senior management, and boards of directors. This fast-paced workshop has been specifically designed to help internal auditors and their organizations meet these new expectations and increase senior management and board satisfaction levels.
The Way Forward: Reinvent Internal Audit

For at least the past decade, internal auditing has been in a state of growth and progressive change. And while it has evolved and advanced significantly, many practitioners nonetheless remain bound by some fundamental, confining paradigms. These paradigms include:

- Internal auditors plan, execute, and report audits of points-in-time audits.
- Internal auditors assess internal controls and report opinions on whether they believe controls are effective.
- Internal auditors report what they believe to be control deficiencies, material weaknesses, significant deficiencies, or opportunities for improvements.
- Direct-report auditing is the primary approach used globally. In a direct-report engagement, the auditor evaluates the subject matter for which the accountable party is responsible. The accountable party does not make a written assertion on the subject matter.
- The profession has been primarily supply-driven rather than demand-driven, as boards and C-teams have often not specified their assurance needs—leaving internal audit departments to form their own views regarding which objective/topic to focus on.
- Internal audit often does not know, or require that management and boards define, the type and amounts of residual risk the company and its board are prepared to accept.

Reinventing Internal Audit

Tim J. Leech

Recent governance-related developments require the profession to revisit some of its long-held paradigms.
The Way Forward:
Reinvent Internal Audit

HOW???
BOARD & C-SUITE
DRIVEN/OBJECTIVE CENTRIC
ERM & INTERNAL AUDIT
END OF MODULE 1

QUESTIONS???

timleech@riskoversightsolutions.com
Audit Transformation Strategies to Meet Escalating Stakeholder Expectations

Module 2: Board & C-Suite Driven/Objective Centric ERM and Internal Audit

Tim Leech, Managing Director
Risk Oversight Solutions Inc.
timleech@riskoversightsolutions.com

www.riskoversightsolutions.com

Mountains of Change...Oceans of Opportunities
Workshop Agenda

Module 2 Board & C-Suite Driven/Objective Centric ("BCD/OC") ERM and IA

- BCD/OC Design Objectives
- BCD/OC Core Elements
- BCD/OC Key Benefits to IA
- BCD/OC Examples
- BCD/OC Tools
- BCD/OC Implementation Barriers
- BCD/OC Implementation Steps & Options
Redefine risk management from being seen primarily hazard avoidance/management to a tool to increase certainty key objectives are achieved while still operating with a tolerable level of retained risk

Provide management and boards with a practical solution to meet escalating board risk oversight and risk governance expectations

Generate higher levels of management and board participation in ERM and internal audit

Put the focus and resources on top value creation and potential value erosion end result objectives
BCD/OC Design Objectives

• Transition organizations from “supply driven” to “board/demand driven” assurance
• Provide a platform to “optimize” risk treatment design (i.e. lowest possible cost combination of risk treatments capable of producing an acceptable residual risk status)
• Integrate the work of all assurance functions including IA, risk, safety, compliance, insurance, legal, and others
BCD/OC Design Objectives

- Elevate the stature of and value added by Internal Audit and ERM support staff
- Integrate strategic planning and ERM
- Engage boards and senior management defining the amount of risk assessment rigor and independent assurance. This is a key risk decision in its own right that hasn’t been sufficiently recognized
- Clarify accountabilities and role of all key assurance players including the board, senior management, work units, ERM staff and internal audit
- Meet emerging risk oversight expectations
Use an “OBJECTIVES REGISTER” with **top value creation/strategic objectives** and **top potential value erosion objectives** as the foundation for all ERM and internal audit work, not a “risk register” or “audit universe”.

<table>
<thead>
<tr>
<th>Corporate</th>
<th>Description</th>
<th>End Result Objective Owner / Sponsor(s)</th>
<th>Composite Residual Risk Rating (CRRR)</th>
<th>CRRR Update Date</th>
<th>Potential to increase Entity Value</th>
<th>Potential to Erode Entity Value</th>
<th>Current Risk Assessment Rigor (RAR)</th>
<th>Independent Assurance Level (IAL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ensure that financial statements are reliable and in compliance with GAAP.</td>
<td>Tim Leech</td>
<td>6 - Major</td>
<td>6/12/2014</td>
<td>Medium</td>
<td>Low</td>
<td>Medium (M)</td>
<td>LOW</td>
</tr>
<tr>
<td>2</td>
<td>Safeguard and enhance ABC’s reputation</td>
<td>Tim Leech</td>
<td>4 - Advanced</td>
<td>6/10/2014</td>
<td>High</td>
<td>High</td>
<td>Very Low (VL)</td>
<td>MEDIUM</td>
</tr>
</tbody>
</table>
BCD/OC Core Elements

“Top potential value erosion objectives” are also called “foundation objectives” and include compliance with laws, reliable external disclosures, safety and other social responsibility objectives.
Engage senior management and the board in the process used to decide which objectives to include in the "OBJECTIVES REGISTER".
Engage senior management and the board in the process used to decide “Risk Assessment Rigor” and “Independent Assurance Level”
B.C./O.C. Core Elements

Conscious and transparent decisions on “Risk Assessment Rigour”

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

Conscious and transparent decisions on “Independent Assurance Level”

**NIA** – No independent assurance

**LOW** – A high level assurance review has been completed and a feedback report provided to the OWNER/SPONSOR and RISK OVERSIGHT COMMITTEE

**MEDIUM** – An independent review has been completed to assess the completeness of risks identified, risk treatments and residual risk status information provided and a report provided to the OWNER/SPONSOR and RISK OVERSIGHT COMMITTEE

**HIGH** – In addition to the steps defined for MEDIUM, steps have been taken to confirm the existence and effectiveness of the risk treatments identified.
Assign primary responsibility to report upwards on the residual risk status linked to each objective to a “OWNER/SPONSOR”
BCD/OC Core Elements

Consider the full range of “Risk Treatments” when completing Risk Treatment Strategy section
BCD/OC Core Elements

Focus on the acceptability of “Residual Risk Status”, specifically whether it is, or is not, within the entity’s risk appetite and tolerance.
BCD/OC Core Elements

Conscious and transparent decisions on “Composite Residual Risk Rating”

**COMPOSITE RESIDUAL RISK RATING DEFINITIONS**

1. **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)

2. **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.

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

4. **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.

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

6. **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.

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

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

9. **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.

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

11. **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.

---

2013 Risk Oversight Inc.
After the decision on acceptability of residual risk status has been made, assess if the Risk Treatment Strategy is “Optimized”
**BCD/OC Core Elements**

Provide consolidated reports on residual risk status to the board

<table>
<thead>
<tr>
<th>Draft objective statement</th>
<th>Owner/Sponsor Candidate</th>
<th>Target Risk Assessment Rigour</th>
<th>Target Independent Assurance Level</th>
<th>Composite Residual Risk Rating</th>
<th>CRRR Update Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure risks related to the ABC’s business model of outsourcing management and advisory services have been identified, assessed and reported to key shareholders</td>
<td>ABC Board</td>
<td>Medium</td>
<td>Medium</td>
<td>TDD</td>
<td>10/01/2015</td>
</tr>
<tr>
<td></td>
<td>ABC Board</td>
<td>Medium</td>
<td>Medium</td>
<td>TDD</td>
<td>10/01/2015</td>
</tr>
<tr>
<td>Ensure the company maintains sufficient critical mass of skilled people to maintain shareholder value over a 10 year period</td>
<td>John Smith</td>
<td>Medium</td>
<td>Medium</td>
<td>TDD</td>
<td>10/01/2015</td>
</tr>
<tr>
<td>Ensure senior management and the board meet or exceed in-house governance requirements for Terence normalized</td>
<td>ABC Board</td>
<td>Medium</td>
<td>Medium</td>
<td>TDD</td>
<td>10/01/2015</td>
</tr>
<tr>
<td>Ensure all financial obligations and covenants are met whilst optimizing the cost of capital and balancing risk and reward</td>
<td>John Miller</td>
<td>Low (target medium)</td>
<td>TBD</td>
<td>TDD</td>
<td>01/02/2015</td>
</tr>
<tr>
<td>Optimize investment portfolio to produce target returns whilst complying with investment guidelines</td>
<td>MF Frederik</td>
<td>Medium</td>
<td>Medium</td>
<td>TBD</td>
<td>01/02/2015</td>
</tr>
<tr>
<td>Ensure that investments comply with the partnership agreement and discourage all actual and potential conflicts of interest</td>
<td>John Miller</td>
<td>Low (target medium)</td>
<td>TBD</td>
<td>TDD</td>
<td>01/02/2015</td>
</tr>
<tr>
<td>Ensure the company complies with all applicable laws and regulations</td>
<td>John Miller</td>
<td>Low (target medium)</td>
<td>TBD</td>
<td>TDD</td>
<td>01/02/2015</td>
</tr>
<tr>
<td>Maintain the ability to operate in the event of a termination of the outsourcing IT service provider</td>
<td>Chuck Clark</td>
<td>Low (target medium)</td>
<td>TBD</td>
<td>TDD</td>
<td>15/07/2014</td>
</tr>
<tr>
<td>Ensure financial statements are reliable and in accordance with IAS and CAS Radnul rules and that investments are included in all</td>
<td>John Miller</td>
<td>Low (target medium)</td>
<td>TBD</td>
<td>TDD</td>
<td>15/07/2014</td>
</tr>
<tr>
<td>Safeguard and enhance the company’s reputation</td>
<td>Ann Peabody</td>
<td>Low (target medium)</td>
<td>TBD</td>
<td>TDD</td>
<td>28/07/2014</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
BCD/OC Key Benefits to IA

- IA focuses on the top value creation and potential value erosion objectives elevating IA’s stature and value add
- Boards and senior management define the level of risk assessment rigor and independent assurance they want. This defines ERM staff and IA’s scope and resources required
- IA staff must learn to consider and assess the full range of “risk treatments” not just “internal controls”
BCD/OC Key Benefits to IA

- IA actively participates in the process of generating the information necessary for management and boards to assess if the current residual risk status is, or is not, within their risk appetite and tolerance (i.e. per the FSB the “Risk Appetite Framework”)

- IA transitions from the business of providing subjective opinions on “control effectiveness” on a small fraction of the risk universe to ensuring senior management and the board are aware of the current residual risk status linked to key strategic value creation objectives and potential value erosion objectives. Conflict and non-productive haggling over wording is reduced significantly
BCD/OC Key Benefits to IA

- IA actively participates in the process of optimizing risk treatment design by providing quality assurance reviews and feedback.

- IA plays a role ensuring that the board is actively participating in the organization’s strategic planning process and meeting escalating risk oversight expectations.

- In organizations with dedicated risk staff their role is to create and maintain the Risk Appetite/risk management framework. IA’s role is to report on the process and reliability of the consolidated report from management on residual risk status.
**Risks**

**Principal Risks, Risk Management and Risk Oversight**

The Board is responsible for managing and overseeing risk. A Board-driven, objective-centric approach to risk management and internal audit has been adopted that focuses on identifying the most critical value creation objectives and potential value erosion risks if an objective is not met; recording these objectives in a corporate objectives register; assigning specific management personnel in ASVG to objectives to regularly assess and report to the Board on the state of retained/residual risk, including whether the current residual risk status is consistent with the Company’s risk appetite; and direct, senior ASVG management and Board input and involvement in deciding which end-result objectives warrant formal risk assessments; and the appropriate level of risk assessment rigour and independent assurance to be applied in light of cost/benefit considerations. The Board believes this approach better positions the Company to meet the emerging risk governance expectations proposed by the Financial Stability Board (FSB) globally, and the Financial Reporting Council (FRC).

---

**Internal control/risk treatment**

The Code requires the Board to at least annually conduct a review of the adequacy of the Company’s...
BCD/OC Examples

Ottawa Humane Society: The first charity in the world to implement BDO/OC
Western University is a licensed user of Risk Oversight Solutions training tools and materials.
BCD/OC Tools

RiskStatusline™

End Result Objective
(implicit or explicit)

Internal/External Context

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

Threats to Achievement/Risks?

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

Risk Treatment Strategy

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?

NO

Re-examine risk
treatment strategy
and/or objective and
develop action plan

YES

Risk Treatment
Optimized?

NO

YES - Move On

YES

Risk Status

Conclusion

RISKSTATUSOVERSIGHT™ QUICK START – Hard copy
laminates, booklets and workbooks

<table>
<thead>
<tr>
<th>Item Description</th>
<th># of Copies</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>RiskStatusline™ Training Diagram and Risk Treatment Principles – double sided</td>
<td></td>
<td></td>
</tr>
<tr>
<td>laminate 2 pages ($10 each)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RiskStatusline™ Quick Reference and RiskStatusline™ Risk Treatment Design Elements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>– double sided laminate 2 pages ($10 each)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RiskStatusline™ Risk Treatment Design Elements Definitions/Trigger Statements –</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11 page booklet ($10 each)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RiskStatusline™ Owner/Sponsor Guide – 7 page booklet ($10 each)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RiskStatusline™ MS Word template – ($10 – electronic copy, only 1 required)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sample BCD/OC Corporate Risk Management Policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>($10 each)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Board &amp; C-Suite Driven/Objective Centric Assurance: Key Concepts and CRRR, RAP,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>and IIA Ratings Definitions – double sided laminate ($10 each)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Workbook: Board &amp; C-Suite Driven/Objective Centric and Internal Audit: Core</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Skills and Implementation Strategies – 150+ pages ($100 each)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Workbook: Facilitating RiskStatusline™: Workshops: Core Skills &amp; Tips for Success</td>
<td></td>
<td></td>
</tr>
<tr>
<td>– 100+ page workbook ($100 each)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Workbook: Completing Audits and Quality Assurance Reviews Using the</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RiskStatusline™ Method: Core Skills &amp; Tips for Success – 100+ page workbook ($100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>each)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RiskStatusline™ complete package including all the documents referenced above</td>
<td></td>
<td></td>
</tr>
<tr>
<td>in hard copy ($400 each)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*shipping and handling will be calculated and added onto your total based on the address provided and an
invoice will be sent to you for order confirmation before final billing. All prices are quoted in U.S. dollars.
Group Discussion

• What barriers do you see that could impede the ability of Internal Audit departments that want to help their organization implement BCD/OC ERM and Internal Audit?
BCD/OC Implementation Barriers

Not all CEOs want their board to be aware of areas of high risk acceptance. Not all boards want to know the whole truth and nothing but the truth.
BCD/OC Implementation Barriers

"Risk cultures" that are not supportive of identifying and disclosing the true state of residual/retained risk
Reluctance to acknowledge that traditional risk-centric/risk register approaches to ERM in use around the world are not working very well
BCD/OC Implementation Barriers

Reluctance to acknowledge that traditional spot-in-time internal audit methods that focus on providing subjective opinions on the “effectiveness” of internal control need to change.
BCD/OC Implementation Barriers

Truly effective ERM discloses information that may increase litigation risk

Dictionary

double-edged sword

noun

: a sword that has two sharp edges
: something that has both good and bad parts or results
BCD/OC Implementation Barriers

In the absence of real and serious pressure to change, human beings often resist rapid radical change.

Calls for Improved Enterprise-Wide Risk Oversight

68% indicate that the board of directors is asking “somewhat” to “extensively” for increased senior executive involvement in risk oversight. That is even higher for large companies (86%) and public companies (88%).

- 65% of organizations experience “somewhat” to “extensive” pressure from external parties to provide more information about risks.
- Financial services organizations are especially experiencing these external pressures with 79% experiencing them “somewhat” to “extensively.” These demands are most notably coming from regulators.

Risk Oversight Leadership

32% have designated an individual to serve as the chief risk officer or equivalent.

- Financial services organizations are most likely to designate an individual as CRO or equivalent, with such appointments occurring in 56% of the firms surveyed.

45% have a management-level risk committee

- For most organizations with a risk management committee, the committee meets at least quarterly.

BCD/OC Implementation Barriers

For non-financial public companies, an absence of serious regulatory pressure to change except in the UK (UK Corporate Governance Code September 2014)

No tangible action since 2009 proxy disclosure rules

No tangible action since 2010 audit report on governance disclosures
Board & C-Suite Driven/Objective Centric ERM and Internal Audit Five Step Overview

1. Populate Objectives Register: top value creation and potential value erosion objectives
   - Step 1
2. Assign objective “Owner/Sponsors”, Risk Assessment, Rigor (RAR) and Independent Assurance Levels (IAL)
   - Step 2
3. Confirm decisions on objectives coverage, EARs, IALs with Board
   - Step 3
4. Owner/Sponsors complete RiskStatuslines™ (RSLs) and IA completes independent assurance work
   - Step 4
5. Consolidated report including Composite Residual Risk Ratings prepared for senior management and the board
   - Step 5
BCD/OC Implementation Options

Go Slow Approach #1 – start by doing some audits using RiskStatus™ method
BCD/OC Implementation Options

Go Slow Approach #2 – run some risk workshops using RiskStatusline™ method
BCD/OC Implementation Options

Go Slow Approach #3 – provide orientation to senior management and your board on risk oversight expectations and alternatives to traditional internal audit and ERM methods and seek input
BCD/OC Implementation Options

Faster Approach #1 – brief senior management and board on the approach and benefits and seek approval for full implementation over 3-5 years – “Mountains of change...Oceans of Opportunities”
End of Module 2

QUESTIONS???
Thank you

timleech@riskoversightsolutions.com