Five Lines of Assurance: A New Paradigm in Internal Audit & ERM

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

www.riskoversightsolutions.com
Speaker Professional Profile

Tim J. Leech, FCPA CIA CRMA CCSA CFE is Managing Director at Risk Oversight Solutions Inc. based in Oakville, Ontario, Canada and Sarasota, Florida. He has over 30 years of experience in the risk governance, internal audit, IT, and forensic accounting/litigation support fields. His experience base includes setting up a new business unit, a “first of its kind”, for Coopers & Lybrand, “Control & Risk Management Services” in 1987; founding in 1991, building, and successfully selling CARD®decisions, a global risk and assurance consulting and software firm, to Paisley/Thomson Reuters in 2004; serving as Paisley’s Chief Methodology Officer from 2004 -2007; and 30+ years of global experience helping clients around the world with internal audit transformation initiatives and the design, implementation, and maintenance of integrated and more powerful ERM/IA 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. Tim was the first in 2009 to develop and deliver training on IIA IPPF Standard 2120 to equip internal auditors to assess and report on the effectiveness of risk management processes. He is the author of the Conference Board Director Notes December 2012 publication “Board Oversight of Management’s Risk Appetite and Tolerance”, co-author of the highly acclaimed January 2014 “Risk Oversight: Evolving Expectations for Boards”, and most recently, “Paradigm Paralysis in ERM and Internal Audit” in the summer 2016 issue of Ethical Boardroom. His ground breaking article, “Reinventing Internal Audit”, published in the April 2015 issue of Internal Auditor magazine has attracted global recognition and was awarded a 2016 Outstanding Contribution Award from IIA global.

In 2013 he launched a second generation of disruptive innovation with a breakthrough approach to risk and assurance management – “Five Lines of Assurance: Board & C-Suite Driven/Objective-centric ERM and Internal Audit”. The goal – respond to the rapid escalation in board risk oversight expectations and deliver substantially more “bang for the buck” from formal assurance spending.

Leech was the recipient of IIA Canada’s first Outstanding Contributions to the Profession award at the first IIA Canada national conference in Quebec City in 2009, and is currently working with IIA Global in Florida to roll-out training on “Five Lines of Assurance/Board & C-Suite Driven/Objective Centric ERM and internal audit to CAEs, IIA National Institutes, and in-house IIA training clients around the world.
Part 1: Escalating Expectations

- Escalating Expectations: Regulators
- Escalating Expectations: Credit Agencies
- Escalating Expectations: Institutional Investors
- Escalating Expectations: Director Associations
- Escalating Expectations: Internal Audit & ERM Customers
- IIA Response to date
- The Way Forward: Five Lines of Assurance - A New Paradigm in ERM & Internal Audit
Part 2 Five Lines of Assurance- A New Paradigm in ERM and IA

- 5LoA Design Objectives
- 5LoA Core Elements
- 5LoA Key Benefits
- 5LoA Examples
- 5LoA Tools
- 5LoA Implementation Overview
Escalating Expectations: Regulators

Guide to Integrated Risk Management

A recommended approach for developing a Corporate Risk Profile

Table of Contents

1. Introduction
   - 1.1 About this Guide
   - 1.2 Background

2. Overview of the TBS Framework for the Management of Risk
   - 2.1 Key Concepts
   - 2.2 About the Framework for the Management of Risk
   - 2.3 Risk Management Principles
   - 2.4 Roles and Responsibilities of Deputy Heads and TBS

3. Integrated Risk Management – Overview

4. Getting Started – Planning and Designing the Approach and Process
   - 4.1 General
   - 4.2 Understanding the Organization and its Context
   - 4.3 Establishing and Articulating Direction for Integrated Risk Management
   - 4.4 Accountability
   - 4.5 Resources
   - 4.6 Defining the Risk Management Process
   - 4.7 Establishing Communications and Reporting Mechanisms

5. Putting It in Place – Implementing Integrated Risk Management
   - 5.1 Implementing the Risk Management Approach and Process
   - 5.2 Providing the Environment and Infrastructure

6. Doing It – Practicing Integrated Risk Management
   - 6.1 Ongoing Integrated Risk Management
   - 6.2 Creating a Corporate View of Risk
   - 6.3 Ensuring Continuous Risk Management Learning

7. Improving It – Continuously Improving integrated Risk Management

8. Contact Information

Appendix A – Interdepartmental Working Group
**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
Financial Stability Board ("FSB") November 2013:

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 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 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;
4.6 Internal audit (or other independent assessor) should:\(^3\):

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, as well as strategic and business planning, compensation, and decision-making processes;

e) assess the design and effectiveness of risk measurement 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.
Board responsibilities per FRC UK Sept 2014 Code

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;
Guide to Integrated Risk Management

A recommended approach for developing a Corporate Risk Profile

Table of Contents

- 1 Introduction
  - 1.1 About this Guide
  - 1.2 Background
- 2 Overview of the TBS Framework for the Management of Risk
  - 2.1 Key Concepts
  - 2.2 About the Framework for the Management of Risk
  - 2.3 Risk Management Principles
  - 2.4 Roles and Responsibilities of Deputy Heads and TBS
- 3 Integrated Risk Management – Overview
- 4 Getting Started – Planning and Designing the Approach and Process
  - 4.1 General
  - 4.2 Understanding the Organization and its Context
  - 4.3 Establishing and Articulating Direction for Integrated Risk Management
  - 4.4 Accountability
  - 4.5 Resources
  - 4.6 Defining the Risk Management Process
  - 4.7 Establishing Communications and Reporting Mechanisms
- 5 Putting It in Place – Implementing Integrated Risk Management
  - 5.1 Implementing the Risk Management Approach and Process
  - 5.2 Providing the Environment and Infrastructure
- 6 Doing It – Practicing Integrated Risk Management
  - 6.1 Ongoing Integrated Risk Management
  - 6.2 Creating a Corporate View of Risk
  - 6.3 Ensuring Continuous Risk Management Learning
- 7 Improving It – Continuously Improving Integrated Risk Management
- 8 Contact Information
- Appendix A – Interdepartmental Working Group
Integrated Risk Management

Risk management cannot be practiced effectively in silos. As a result, *integrated* risk management promotes a continuous, proactive and systematic process to understand, manage and communicate risk from an organization-wide perspective in a cohesive and consistent manner. It is about supporting strategic decision-making that contributes to the achievement of an organization's overall objectives. It requires an ongoing assessment of risks at every level and in every sector of the organization, aggregating these results at the corporate level, communicating them and ensuring adequate monitoring and review. Integrated risk management involves the use of these aggregated results to inform decision-making and business practices within the organization.

Deputy Heads

Deputy Heads are responsible for managing their organization's risks by leading the implementation of effective risk management practices, both formal and informal. This includes establishing the organization’s overall risk management approach and ensuring that supporting processes are in place. In doing so, Deputy Heads are encouraged to apply the principles outlined in section 2.3. A key role of the Deputy Head is to ensure that risk management principles and practices are understood and integrated into the various activities of his/her organization. Deputy Heads are also responsible for monitoring risk management practices in their organizations, as well as considering risks that arise when partnering with organizations within and external to the federal public service. This includes ensuring that issues affecting the organization's risk management approach, whether identified through assessments or internal and external monitoring, are examined, reviewed and addressed effectively. In addition, Deputy Heads play an important role in creating a learning environment that promotes continuous improvement in risk management competencies and capacity within their organization. Through their leadership, Deputy Heads foster a risk-informed organizational culture that supports risk-informed decision-making, enables dialogue on risk tolerance, focuses on results and enables the consideration of both opportunity and innovation.

Generally, there are numerous tools and techniques for analyzing (e.g. workshops, surveys) and prioritizing (e.g. risk maps) risks. Organizations are encouraged to design a process that is appropriate for their own operating environment. In defining risk assessment activities within the risk management process, organizations may wish to provide direction regarding:

• who should be involved in the assessment of risks;
• how much rigour is required for a particular risk assessment exercise;
• what type of information needs to the collected and what level of detail is required; and
• how assessed risks should be documented for response purposes.

Escalating Expectations: Credit Agencies

Global Credit Portal
RatingsDirect

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

Primary Credit Analyst:
Steven J. Dugas, New York (212) 406-7187, steven_dugas@standardandpoors.com

Table Of Contents

Frequently Asked Questions

www.standardandpoors.com/ratingsdirect

Special Comment

Best Practices for a Board’s Role in Risk Oversight

Summary

Moody’s views a board of directors’ risk oversight role as critical to the sound running of an organization — especially for financial institutions and for other companies with significant market and credit risk exposure. In particular, Moody’s sees high expectations for boards’ role in shaping a firm’s risk appetite and assessing a proper risk management framework. This is especially true for firms with a dual board structure. In this context, Moody’s emphasizes the need for a clear and effective risk management framework.

The special comment discusses the principles guiding the role of boards on risk oversight. Moody’s views these practices as essential to the role of the board. This special comment highlights the importance of risk management frameworks in the context of corporate governance. For further details, please consult the full report for a comprehensive analysis.
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: Director Associations

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
Haydeneck & Struggles International, Inc.
KPMG's Audit Committee Institute
Oliver Wyman
Pearl Meyer & Partners
Tatum, LLC
Weil, Gotshal & Manges LLP

NATIONAL ASSOCIATION OF CORPORATE DIRECTORS

A FRAMEWORK FOR BOARD OVERSIGHT OF ENTERPRISE RISK

by John E. Caldwell, CPA, CA
Escalating Expectations: IA Customers

Evolution or irrelevance?
Internal Audit at a crossroads

Deloitte's Global Chief Audit Executive Survey
www.deloitte.com/globalICAEsurvey
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.
IIA Response to Date

To Be "Agents of Change," Internal Auditors Must Embrace Change

Richard Chambers  February 29, 2016  0 Comments

One of my favorite quotes in motivating internal auditors of the urgency to change when warranted is drawn from the Danish philosopher Soren Kierkegaard, who noted, “All change is preceded by crisis.” While I do not believe the profession faces a full-blown crisis in 2016, there are certainly imperatives to change as there always are for professions that are growing and evolving.

A great resource to gauge what those imperatives are is The IIA’s annual North American Pulse of Internal Audit from the Audit Executive Center, which has become an important tool for CAEs who have come to rely on its trend data.

Data in the recently released Pulse report reflects the continuing evolution in our profession – particularly the trend toward financial and compliance audits making up less of the audit plan (down 10 percent since 2012) and the steady growth in the percentage of CAEs reporting functionally to audit committees or boards (up 7 percent since 2013 to 83 percent).

These two trends reflect much bigger changes in the profession that manifest themselves in varied ways. As risk in the marketplace becomes more dynamic and complex, stakeholders are turning to internal audit to apply their deep knowledge of the organization to the emerging risks it faces. As pressures on boards and audit committee members grow, audit committee members recognize the direct reporting line helps them gain greater assurance and insight on the effectiveness of risk management and control within the enterprise.

We must acknowledge that the same factors driving those two trends create new demands on internal audit practitioners. The key message of this year’s Pulse, “Time to Move out of the Comfort Zone” addresses four areas where these new demands are peaking — cybersecurity, data analytics, auditing culture, and developing interpersonal skills. While the title of the 2016 Pulse might seem a bit provocative, even ominous, I see this as an opportunity to clearly define where the profession must go to grow and succeed — and avoid the “real crisis” that Kierkegaard spoke of.

As stakeholders call on internal audit to do more, the profession must be prepared to invest in the talent, training, and tools necessary to meet those demands. The report’s conclusion includes this prescient observation, “It is time for internal audit to move beyond being capable of handling old risks and align with the strategic objectives of the organization, stepping into the role of trusted advisor.”

I have written that the history of our proud profession reflects that we do not shrink from new challenges. Indeed, we thrive on them. Encourage readers of the Pulse to take its message to heart and develop a step-by-step plan to move out of your comfort zones. Here are a few suggestions to get you started.

Carefully examine the data from each of the four focus areas covered in the Pulse report. In addition to providing valuable data gleaned from a survey of 486 CAEs, directors, and senior managers, the Pulse lays out clearly the challenges practitioners face in the four focus areas and arms you with data to help understand and address them.
For at least the past decade, internal auditing has been in a state of growth and progressive change. Although it has evolved and advanced significantly, many practitioners nonetheless remain bound by some fundamental, confusing paradigms. These paradigms include:

- Internal auditors plan, execute, and report results of point-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 improvement.
- Direct-reporting 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-suite have often not specified their assurance needs—leaving internal audit departments to form their own views regarding which objectives/topics 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.

Recent governance-related developments require the profession to revisit some of its long-held paradigms.
Three Lines of Defense versus Five Lines of Assurance

Elevating the Role of the Board and CEO in Risk Governance

Tim J. Leech
Managing Director, Risk Oversight Solutions Inc.

Lauren C. Hanlon
Director, Risk Oversight Solutions Inc.

Business leaders are continuously exposed to a multitude of ideas, theories, and models that all claim will help them do a better job. One of the current trending corporate governance models that many boards of directors have been exposed to already, or will be soon, is called the three lines of defense model. The global Institute of Internal Auditors (IIA), national regulators, risk management associations, major consulting firms, and others are aggressively promoting and rallying behind it. On the legal front, they are starting to legislate it. A groundswell of global support for this model is building. Be warned however, this chapter and its authors offer a word of caution—the three lines of defense model is based on traditional governance methods and ideas that have not worked well in countless corporate governance scandals that have emerged over the past 30 years, and it does not respond well to emerging expectations that call on CEOs and boards to more actively and visibly participate in and oversee their company's risk governance framework.
The Way Forward: Paradigm Shift Required

Paradigm paralysis in ERM & internal audit

Boards and CEOs around the world are being told repeatedly from multiple sources that they need to do a better job managing and overseeing risk, and, most recently, “risk culture.” Unfortunately, current methods of providing stakeholders with assurance that risk management processes are effective are fundamentally the same methods that have been used for decades.

The 2008 global crisis is a graphic illustration of their inability to cope with an increasingly fast-moving and complex world. This article is a call to boards, CEOs, line execs, regulators, investor groups and others to make a paradigm shift in risk management and assurance thinking to enable a more proactive and better, more shareholder-friendly stance.

Paradigm paralysis in the enterprise risk management (ERM) and internal audit communities fosters their inability to see new methods available to better meet the needs of stakeholders. This article will outline steps that depict individual risks in terms of likelihood and consequence. Risk heat maps may or may not depict residual risk, the risk remaining after considering risk response/risk treatments as a single risk. These risk heat maps are typically maintained by ERM specialists or internal audit groups and results are reported upwards to the board.

The internal audit profession needs to reinvent itself to better respond to the emerging expectations facing senior management and boards. ERM and internal audit paradigms describe why the current paradigms are failing to keep up with today’s fast-paced business environment and call for new risk management and assurance models.

Paradigm paralysis: ERM methods

Although there is wide variation in how companies have implemented ERM, the most common feature is the creation and maintenance of “risk register” as a foundation. The actual risk registry is linked to the company’s business objectives and strategies ranging from the most strategic to the most operational, a range that is too broad to cover all possible risks. The role of ERM is to provide a framework for identifying and managing a comprehensive range of risks, including strategic, financial, operational, and compliance risks.

Paradigm paralysis: Audit methods

Auditors are called upon to provide numerous services to the company, including financial statement audits, internal control audits, and compliance audits. These audits have become more demanding and time-consuming, and the need for an audit approach that is more focused is critical. The current methods of providing assurance to stakeholders are not effective in identifying and managing risks. The need for an audit approach that is more strategic and risk-focused is critical.

ERF paradigm framework

The primary drawback of the risk-centric ERM paradigm is that it lacks an ability to translate the company’s top-level objectives and control objectives into risk-relevant objectives. This approach does not allow decision makers to see the current state of residual risk linked to the achievement of the company’s most important objectives.

All of these factors, in combination with the lack of a risk-centric approach, create a paradigm paralysis in the internal audit profession. This paralysis is caused by the inability of the current risk management and assurance models to effectively identify, measure, and manage risks. The risk heat maps are not effective in identifying and managing risks, and the current methods of providing assurance to stakeholders are not effective in identifying and managing risks.

Paradigm paralysis: Risk heat maps

Risk heat maps are not effective in identifying and managing risks. The current methods of providing assurance to stakeholders are not effective in identifying and managing risks. The need for an audit approach that is more strategic and risk-focused is critical.

Paradigm paralysis: Risk appetite

The current methods of providing assurance to stakeholders are not effective in identifying and managing risks. The need for an audit approach that is more strategic and risk-focused is critical.

Paradigm paralysis: Risk tolerance

The current methods of providing assurance to stakeholders are not effective in identifying and managing risks. The need for an audit approach that is more strategic and risk-focused is critical.

Paradigm paralysis: Risk management

The current methods of providing assurance to stakeholders are not effective in identifying and managing risks. The need for an audit approach that is more strategic and risk-focused is critical.

Paradigm paralysis: Risk response

The current methods of providing assurance to stakeholders are not effective in identifying and managing risks. The need for an audit approach that is more strategic and risk-focused is critical.

Paradigm paralysis: Risk communication

The current methods of providing assurance to stakeholders are not effective in identifying and managing risks. The need for an audit approach that is more strategic and risk-focused is critical.

Paradigm paralysis: Risk governance

The current methods of providing assurance to stakeholders are not effective in identifying and managing risks. The need for an audit approach that is more strategic and risk-focused is critical.
5LoA Design Objectives

• Redefine risk management from being seen primarily as 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
5LoA 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
5LoA 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”
“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”
## 5LoA Core Elements

Conscious and transparent decisions on “Risk Assessment Rigor/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 risk treatments in place/use for all, or some, of the risks have been identified and documented. Performance and impact information for the objective has been obtained and documented. Data has been updated within the past 12 months.</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 RiskStatusline™ 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 RiskStatusline™ data elements, more advanced techniques to determine velocity of risks, leading/lagging risk indicators, steps taken to assess the reliability of likelihood and consequence ratings and other advanced risk assessment techniques</td>
</tr>
</tbody>
</table>
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"
Consider the full range of “Risk Treatments” when completing Risk Treatment Strategy section.
5LoA 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.
5LoA Core Elements

Conscious and transparent decisions on “Composite Residual Risk Rating”

---

**COMPOSITE RESIDUAL RISK RATING DEFINITIONS**

<table>
<thead>
<tr>
<th>Rating</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fully Acceptable</td>
<td>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.</td>
</tr>
<tr>
<td>Minor</td>
<td>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.</td>
</tr>
<tr>
<td>Moderate</td>
<td>Inaction could result in or allow continuation of mid-level negative impacts. Moderate senior management attention is required to adjust composite residual risk status to an acceptable level.</td>
</tr>
<tr>
<td>Advanced</td>
<td>Inaction could allow continuation of (or exposure to) serious negative impacts. Senior management attention is required to adjust composite residual risk status.</td>
</tr>
<tr>
<td>Significant</td>
<td>Inaction could result in or allow continuation of very serious entity level negative impacts. Senior management attention is urgently required to adjust composite residual risk status to an acceptable level.</td>
</tr>
<tr>
<td>Major</td>
<td>Inaction could result in or allow continuation of very major entity level negative consequences. Analysis and corrective actions are required to adjust composite residual risk status.</td>
</tr>
<tr>
<td>Critical</td>
<td>Inaction virtually certain to result in or allow continuation of very major entity level negative consequences. Analysis and corrective actions are required to adjust composite residual risk status.</td>
</tr>
<tr>
<td>Severe</td>
<td>Inaction virtually certain to result in or allow continuation of very severe negative impacts. Senior management board level attention is urgently required to adjust composite residual risk status.</td>
</tr>
<tr>
<td>Catastrophic</td>
<td>Inaction could result in or allow continuation of catastrophic proportionate impacts. Senior management board level attention is urgently required to adjust composite residual risk status so that it avoids catastrophic negative impacts on the organization.</td>
</tr>
<tr>
<td>Terminal</td>
<td>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 is required to prevent the demise of the entity.</td>
</tr>
</tbody>
</table>
5LoA Core Elements

After the decision on acceptability of residual risk status has been made, assess whether the Risk Treatment strategy is Optimized.
## 5LoA 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>CRIR Update Date</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure risks related to the ABC's business model or outsourcing management and advisory services have been identified, assessed and reported to key shareholders. Provide a liquid, balanced, single-point access to private equity and private equity related assets.</td>
<td>ABC Board</td>
<td>Medium</td>
<td>Medium</td>
<td>TBD</td>
<td>10/01/2015</td>
<td>Completed</td>
</tr>
<tr>
<td>Ensure the company maintains sufficient critical mass of steel to enable operations to maintain above liquidity capital market visibility whilst maximizing short and long-term value for shareholders and enhancing shareholder base. Deliver returns that are more closely related to performance over public market over 10 years.</td>
<td>John Smith</td>
<td>Medium</td>
<td>Medium</td>
<td>TBD</td>
<td>15/07/2015</td>
<td>Completed</td>
</tr>
<tr>
<td>Ensure senior management and the board meet or exceed internal governance requirements for Tokyo listed public.</td>
<td>ABC Board</td>
<td>Medium</td>
<td>Medium</td>
<td>6</td>
<td>31/08/2018</td>
<td>Completed</td>
</tr>
<tr>
<td>Safeguard ABC against fraud. Ensure the risk reward trade-off relating to appropriate contractual provisions and insurance are understood and risk is optimized.</td>
<td>John Miller</td>
<td>Low (target medium)</td>
<td>TBD</td>
<td>TBD</td>
<td>03/02/2015</td>
<td>Further work required, Complete, subject to</td>
</tr>
<tr>
<td>Ensure that all financial obligations and covenants are met whilst optimizing the cost of capital and balancing risk and reward.</td>
<td>John Miller</td>
<td>Medium</td>
<td>Medium</td>
<td>TBD</td>
<td>04/02/2015</td>
<td>Completed</td>
</tr>
<tr>
<td>Optimize investment portfolio to produce target returns whilst conforming with investment guidelines.</td>
<td>MF Frederik</td>
<td>Medium</td>
<td>Medium</td>
<td>TBD</td>
<td>04/02/2015</td>
<td>Completed Further work required</td>
</tr>
<tr>
<td>Ensure that all investments comply with the partnership agreement and address all actual and potential conflicts of interest.</td>
<td>John Miller</td>
<td>Low (target medium)</td>
<td>TBD</td>
<td>TBD</td>
<td>07/03/2015</td>
<td>Completed Further work required</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>TBD</td>
<td>05/03/2014</td>
<td>Further work required Recommendation to delist</td>
</tr>
<tr>
<td>Maintain the ability to operate in the event of a termination of the IT services provider.</td>
<td>Chuck Clark</td>
<td>Low (target medium)</td>
<td>TBD</td>
<td>TBD</td>
<td>16/09/2014</td>
<td>New, Incomplete Completed, subject to</td>
</tr>
<tr>
<td>Ensure financial statements are reliable and in accordance with IAS and CEA standards and that investments are included at all times.</td>
<td>John Miller</td>
<td>Low (target medium)</td>
<td>TBD</td>
<td>TBD</td>
<td>15/07/2014</td>
<td>Completed, subject to</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>TBD</td>
<td>20/08/2014</td>
<td>Completed, subject to</td>
</tr>
</tbody>
</table>
5LoA Key Benefits

• Boards are provided with a concise enterprise level report on the state of residual risk for the company’s top value creation and potential value erosion objectives

• The work of the “assurance silos” including IA, risk, safety, environment, compliance, legal, insurance and others is integrated

• Key information is provided to senior management and the board to assess if the current residual risk status linked to top objectives is, or is not, within the company’s risk appetite/tolerance
5LoA Key Benefits

- Boards are provided with a tangible vehicle to demonstrate they are actively overseeing the company’s “risk appetite framework” (“RAF”)
- The process is designed to fully integrate with strategic planning, new product/service initiatives, and M&A activities.
- The process provides a clear response to emerging expectations like the UK Governance Code, Canadian Securities Administrators, SEC, FSB, credit agencies, institutional investors and TSB.
- The main role of internal audit is to report on the effectiveness of the risk management processes and the consolidated report on residual risk status the board receives from the CEO or his/her designate and to help the company build and maintain robust risk management processes
5LoA Key Benefits

• Boards are provided with a tangible vehicle to demonstrate they are actively overseeing the company’s “risk appetite framework” (“RAF”)
• The process is designed to fully integrate with strategic planning, new product/service initiatives, and M&A activities.
• The process provides a clear response to emerging expectations like the UK Governance Code, Canadian Securities Administrators, SEC, FSB, credit agencies, institutional investors and TSB.
• The main role of internal audit is to report on the effectiveness of the risk management processes and the consolidated report on residual risk status the board receives from the CEO or his/her designate and to help the company build and maintain robust risk management processes
Generally, there are numerous tools and techniques for analyzing (e.g. workshops, surveys) and prioritizing (e.g. risk maps) risks. Organizations are encouraged to design a process that is appropriate for their own operating environment. In defining risk assessment activities within the risk management process, organizations may wish to provide direction regarding:

- who should be involved in the assessment of risks;
- how much rigour is required for a particular risk assessment exercise;
- what type of information needs to be collected and what level of detail is required; and
- how assessed risks should be documented for response purposes.

5LoA Examples

Risk and audit oversight

With the growing sophistication of the UK Corporate Governance Code and significantly heightened investor and regulator risk governance expectations, the SVG Capital Board has adopted a revised approach to risk governance with the following objectives:

- Increase certainty/reduce uncertainty that the Company’s objectives will be achieved while operating within management and the Board’s risk appetite and tolerance.
- Ensure risk assessments clearly link the Company’s key strategic objectives, risks, risk treatments, and Key Performance Indicators (KPIs).
- Ensure the Company’s risk culture continues to be appropriate.
- Increase the direct, visible involvement of the Company’s Board and management in assessing and managing risks of all types to the Company’s top objectives.
- Meet and exceed the governance requirements in the UK Corporate Governance Code.
- Seek to improve our external risk governance communications.

Board

- Determines risk appetite and risk framework
- Responsible for ensuring appropriate risk management framework is in place
- Considers principal risks and uncertainties in detail
- Oversees operation of risk management framework and acceptability of residual risk linked to business objectives
- Detailed review of risk matters at annual strategy Board meeting and periodic reviews at other meetings

Independent risk oversight provider

Chief Executive

- Overall responsibility for building and maintaining robust risk management processes and delivering reliable and timely information on the current residual risk status linked to objectives to the Board. This includes ensuring objectives are assigned owners and sponsors who have primary responsibility to report on the risks.

Risk Management Committee

- Delegated responsibility for risk management
- Ensures appropriate risk management arrangements, processes and techniques in place
- Monitors adherence to risk appetite and risk management framework
- Lobbies with independent risk oversight provider
- Meets at least quarterly

Managers and Other Employees

- Key managers and employees are assigned owner or sponsor responsibility for reporting on objectives not assigned to Chief Executive or Board.
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.
5LoA Tools

Do you know where your Risk is? It's time for a better approach to Risk...

New risk oversight expectations are emerging for Boards, CEOs and CFOs— with escalating pressure from regulators, rating agencies, director associations and shareholders.

Risk Oversight Solutions offers the radically better Five Lines of Assurance approach to risk governance that we call Board & C-Suite Driven/Objective-Centric ERM & Internal Audit. The Five Lines of Assurance approach helps organizations implement specific and practical roles for work units, risk specialist groups, CEOs and the C-Suite, internal audit, and most importantly the Board of Directors. Our approach has been specifically designed to help companies and their boards meet emerging risk governance requirements and fully integrate strategic planning processes and risk management efforts.

Call us for help or purchase one of our cost-effective solutions today:

For companies and public sector organizations—purchase a cost-effective do-it-yourself, worldwide license for the globally acclaimed Five Lines of Assurance/Board & C-Suite Driven/Objective-Centric RiskStatusOversight™ library materials and support, including sample board/management briefings, policies, reference aids, training materials with guidance and support from a Risk Oversight thought leader. Rights to the full library of reference materials are $1/employee with a $5000 U.S. minimum license. Download and browse the RiskStatusOversight™ training and reference aid library here. Additional details are available via the papers and presentations in the New Publication Release section at right.

For registered charities—licences for registered charities start at $1 – it’s our contribution to creating a better world.

For consulting firms—board & c-suite driven/objective-centric distributor licences for ERM and internal audit service providers include support, training materials and reference aids.

More and more, Boards and CEOs are on the hook. Know your risk—for increased investor confidence and better risk treatment. Time for a better response to risk – Call us today.
5LoA Implementation Overview

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, RARs, 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

© Risk Oversight Solutions Inc.
QUESTIONS???
Thank you

timleech@riskoversightssolutions.com