risk oversight solutions

A better response to risk.

Three Lines of Defense vs. Five Lines of Assurance

Elevating the Role of the Board and CEO in Risk Governance

Tim Leech, Managing Director
Risk Oversight Solutions Inc.

Lauren Hanlon, Director
Risk Oversight Solutions Inc.

www.riskoversightsolutions.com

Speaker Professional Profile

Tim J. Leech, FCPA CIA CRMA CCSA CFE

Managing Director at Risk Oversight Solutions Inc.

Leech 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 25+ 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 more recently, "The Next Frontier: Board Oversight of Risk Culture". Leech was a pioneer in the global control and risk self-assessment ("CRSA/CSA") movement from 1996 to 2004. His ground breaking article, "Reinventing Internal Audit" published in the April 2015 issue of Internal Auditor magazine and "Three Lines of Defense versus Five Lines of Assurance": Elevating the Role of the Board and CEO in the May 2016 Wiley/Leblanc Wiley/Leblanc Handbook of Board Governance: A Comprehensive Guide for Public, Private and Not for Profit Board Members, have attracted global recognition.

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 awarded his Fellow designation from the Canadian CPA association in 1997 for distinguished contributions to the profession. He 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.

ro risk oversight solutions
A better response to risk.

Speaker Professional Profile

Lauren Hanlon CPA CA CIA CFE CRMA

Director at Risk Oversight Solutions Inc.

Lauren Hanlon has spent over 20 years providing insight on risk management, internal audit and internal controls for public and private companies in various industries. As the former Director, Internal Audit & Risk at COM DEV International Ltd. (recently acquired by Honeywell International), Lauren Hanlon had oversight of the internal audit, enterprise risk, and compliance and ethics programs, including anti-corruption compliance. She was also an integral member of the Risk Performance & Audit group at BlackBerry as Senior Manager, developing innovative internal audit and risk management solutions for her internal clients.

Her expertise lies in internal audit, risk management and corporate governance, and the development of innovative ERM/IA/SOX software and training modules. Lauren has provided innovative solutions and a fresh approach to ERM methodology and technology training for numerous organizations and risk specialists, including the Big 4 audit partners, in countries around the world. She played an important role in the development and testing of one of the world's first enterprise risk management software platforms, CARDmap, as well as developing globally acclaimed risk and control assessment training materials.

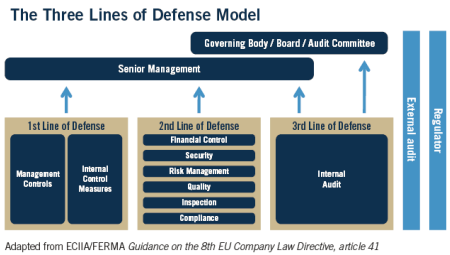
She co-authored a publication *Sarbanes – Oxley and the Canadian Response* for the Richard Ivey School of Business (2005), as well as co-authoring *Preventing the Next Wave of Unreliable Financial Reporting: Why US Congress Should Amend Section 404 of the Sarbanes- Oxley Act,* published in the International Journal of Disclosure & Governance (2011). Most recently she was the co-author of the May 2016 paper *Three Lines of Defense versus Five Lines of Assurance: Elevating the Role of the Board and CEO* in the Wiley/Leblanc *Handbook of Board Governance: A Comprehensive Guide for Public, Private and Not for Profit Board Members*.

She has also lectured at University of Toronto, Continuing Studies Internal Audit Program and has sat on the board of non-profit organizations, including St. Jerome's University.

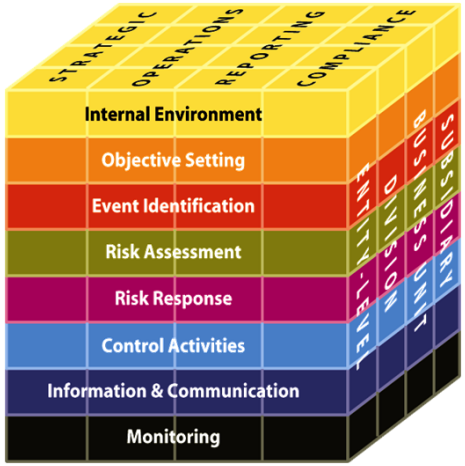
Presentation Agenda

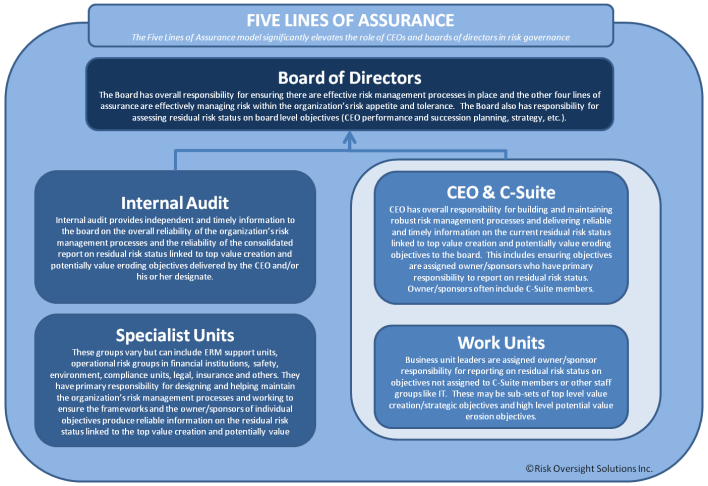
- Introduction: Why care about governance frameworks?
- Overview of Three Lines of Defense (3LoD)
- What's wrong with 3LoD?
- Overview of Five Lines of Assurance (5LoA)
- 5LoA: Core Elements
- 5LoA: Key Benefits
- 5LoA: Why haven't the IIA and risk associations supported 5LoA?
- 5LoA: A Case Study
- 5LoA: Perspectives from the field
- 5LoA: The future

Why care about governance frameworks?



Adapted from ECIIA/FERMA *Guidance on the 8th EU Company Law Directive, article 41*

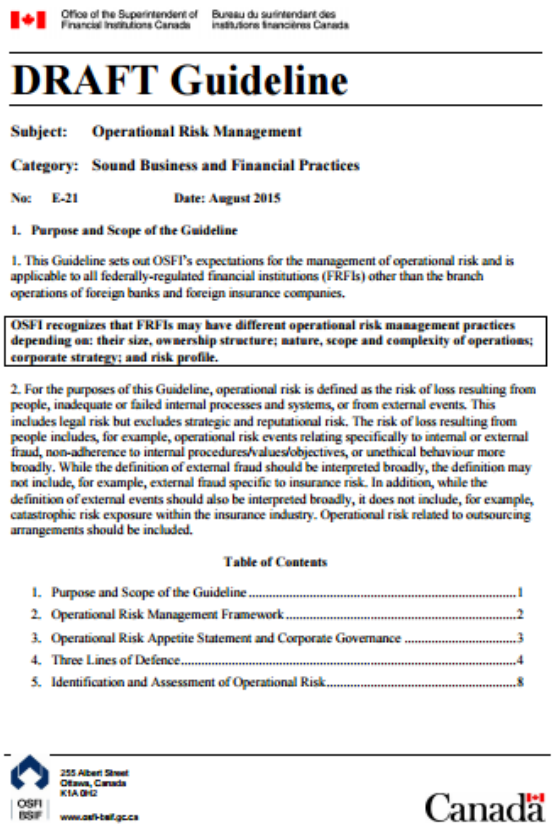




risk oversight solutions
A better response to risk.

Why care about governance frameworks?

SOMETIMES THEY ARE LEGISLATED



Office of the Superintendent of Financial Institutions Canada | Bureau du surintendant des institutions financières Canada

DRAFT Guideline

Subject: Operational Risk Management

Category: Sound Business and Financial Practices

No: E-21 **Date:** August 2015

1. Purpose and Scope of the Guideline

1. This Guideline sets out OSFI's expectations for the management of operational risk and is applicable to all federally-regulated financial institutions (FRFIs) other than the branch operations of foreign banks and foreign insurance companies.

OSFI recognizes that FRFIs may have different operational risk management practices depending on: their size, ownership structure; nature, scope and complexity of operations; corporate strategy; and risk profile.

2. For the purposes of this Guideline, operational risk is defined as the risk of loss resulting from people, inadequate or failed internal processes and systems, or from external events. This includes legal risk but excludes strategic and reputational risk. The risk of loss resulting from people includes, for example, operational risk events relating specifically to internal or external fraud, non-adherence to internal procedures/values/objectives, or unethical behaviour more broadly. While the definition of external fraud should be interpreted broadly, the definition may not include, for example, external fraud specific to insurance risk. In addition, while the definition of external events should also be interpreted broadly, it does not include, for example, catastrophic risk exposure within the insurance industry. Operational risk related to outsourcing arrangements should be included.

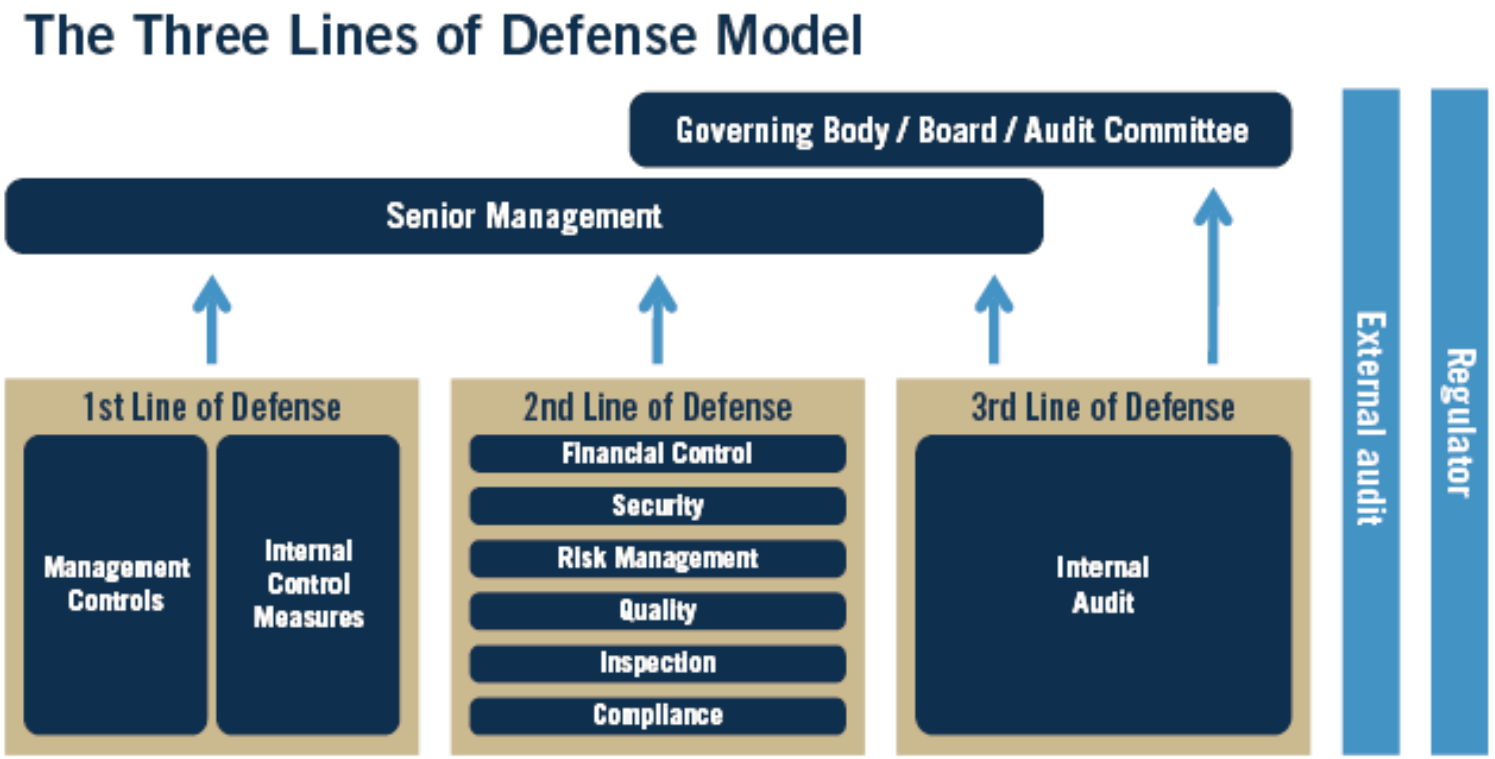
Table of Contents

255 Albert Street
Ottawa, Canada
K1A 0H2
www.osfi-bsif.gc.ca

Canada

risk oversight solutions
A better response to risk.

Overview of 3LoD



Adapted from ECIIA/FERMA *Guidance on the 8th EU Company Law Directive, article 41*

risk oversight solutions
A better response to risk.

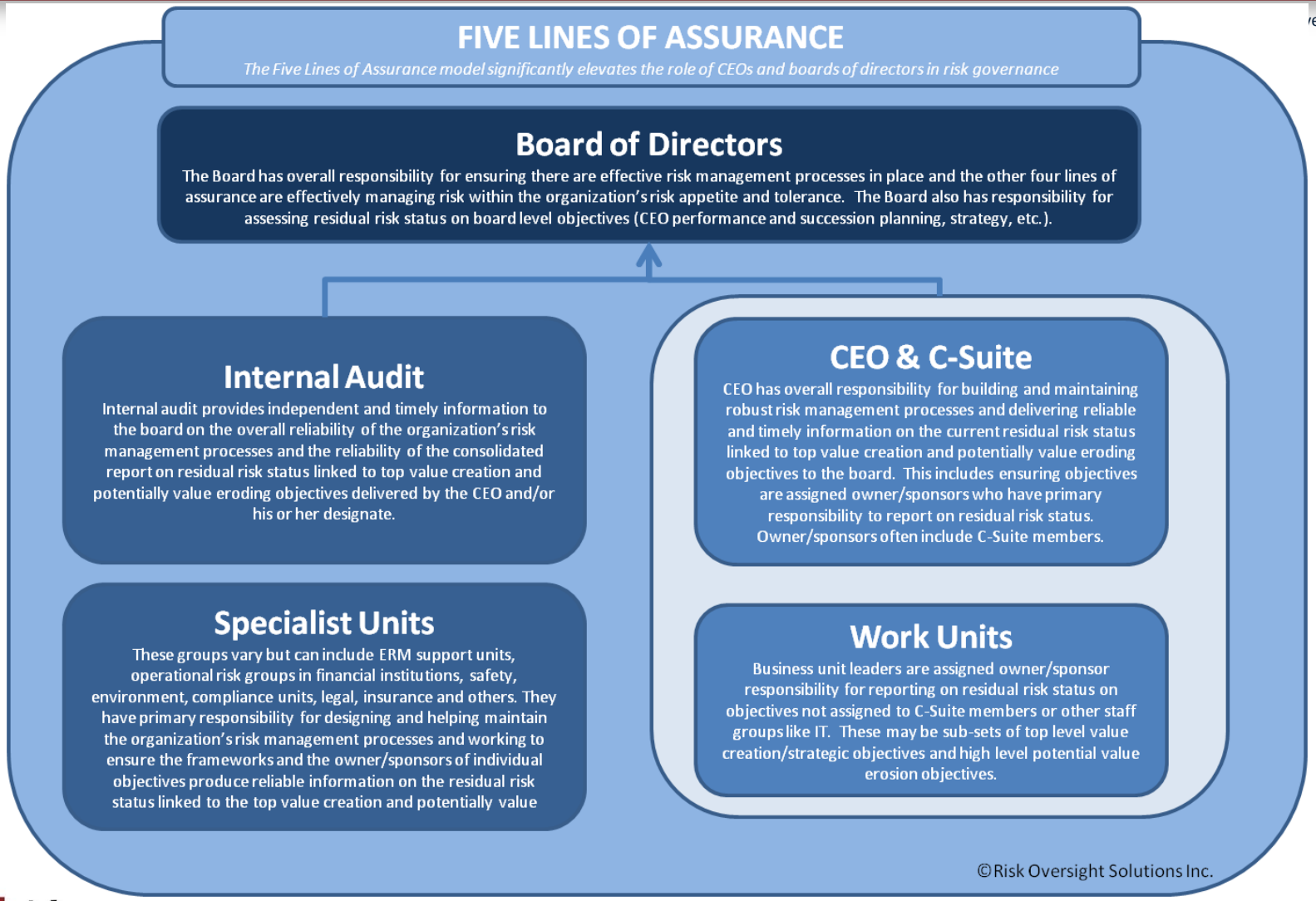
What's wrong with 3LoD?

- It does not recognize and elevate the key role of the board and CEO in effective risk governance – **3LoD sees the board and senior management as "stakeholders" not active and key participants in the risk governance process**
- Perpetuates the notion that risk management is fundamentally about hazard avoidance and defense – not a key support aid to take risks intelligently and drive increased stakeholder value
- Does not support the key concept that risk management, done well, helps senior management and the board make better resource allocation decisions
- Does not support the ISO 31000 definition that the definition of risk is "the effect of uncertainty on the achievement of objectives"

What's wrong with 3LoD?

- Does not elevate/support the concept that the **first line** should not only be responsible for risk and control, they should be responsible for **assessing and reporting on the status of residual risk upwards to senior management and the board**
- Does not clearly communicate that **internal audit** should be **regularly reporting on the effectiveness of the organization's risk management framework**, including the reliability of the consolidated report on the state of residual risk from senior management
- Does not clearly communicate that the role of the **second line** should be focused on helping the first line do a **better job at assessing and reporting on the state of residual risk** to senior management and the board

Overview of 5LoA



5LoA: Core elements

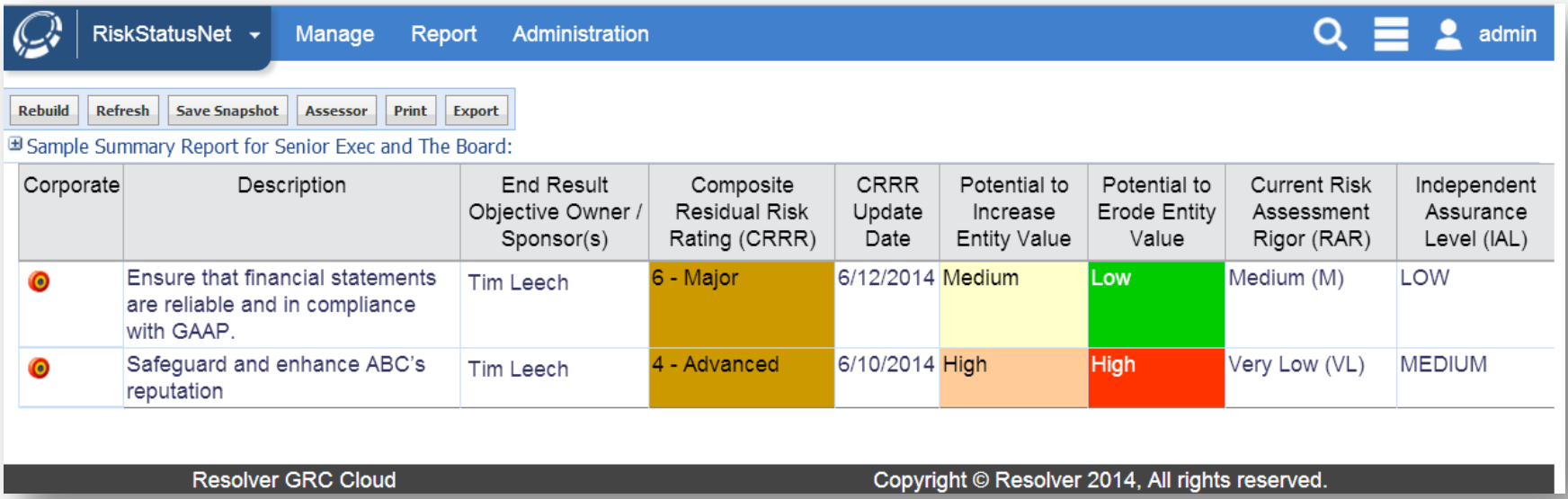
Active board/senior management involvement and clarity around their responsibility as the

‘ultimate line of defense’

risk oversight solutions
A better response to risk.

5LoA: Core elements

Uses an objective register as a foundation not an "audit universe" or "risk register"



Corporate	Description	End Result Objective Owner / Sponsor(s)	Composite Residual Risk Rating (CRRR)	CRRR Update Date	Potential to Increase Entity Value	Potential to Erode Entity Value	Current Risk Assessment Rigor (RAR)	Independent Assurance Level (IAL)
	Ensure that financial statements are reliable and in compliance with GAAP.	Tim Leech	6 - Major	6/12/2014	Medium	Low	Medium (M)	LOW
	Safeguard and enhance ABC's reputation	Tim Leech	4 - Advanced	6/10/2014	High	High	Very Low (VL)	MEDIUM

risk oversight solutions
A better response to risk.

5LoA: Core elements

Clear accountability on who is responsible for reporting on residual risk status

RiskStatusNet | Manage | Report | Administration | admin

Rebuild | Refresh | Save Snapshot | Assessor | Print | Export

Sample Summary Report for Senior Exec and The Board:

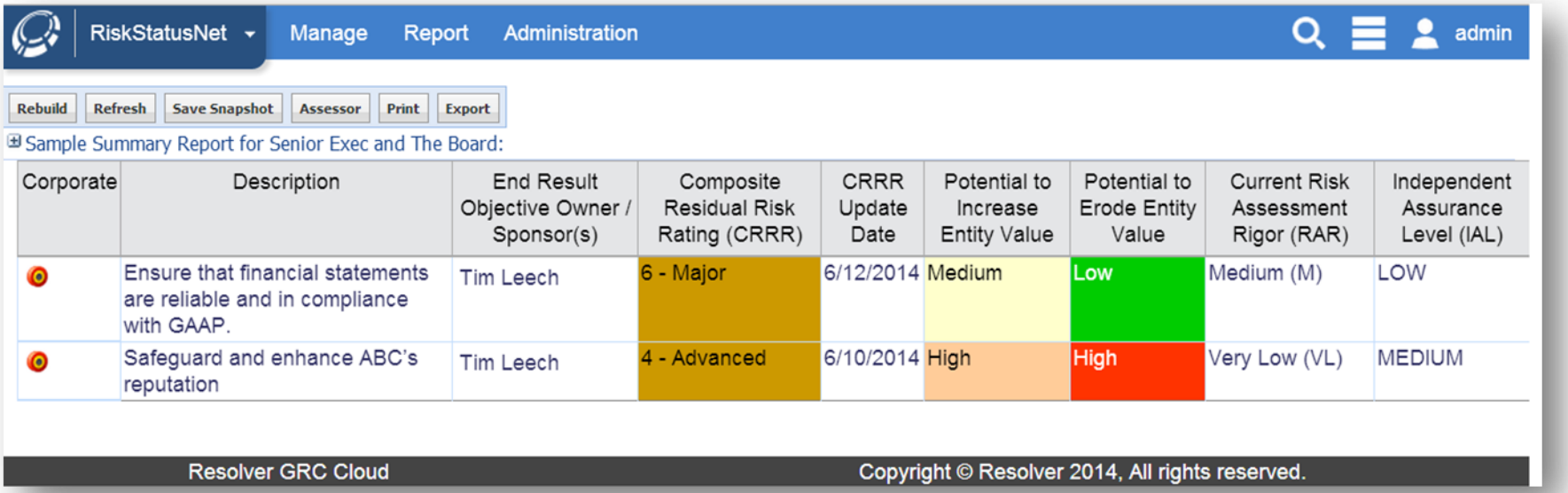
Corporate	Description	End Result Objective Owner / Sponsor(s)	Composite Residual Risk Rating (CRRR)	CRRR Update Date	Potential to Increase Entity Value	Potential to Erode Entity Value	Current Risk Assessment Rigor (RAR)	Independent Assurance Level (IAL)
	Ensure that financial statements are reliable and in compliance with GAAP.	Tim Leech	6 - Major	6/12/2014	Medium	Low	Medium (M)	LOW
	Safeguard and enhance ABC's reputation	Tim Leech	4 - Advanced	6/10/2014	High	High	Very Low (VL)	MEDIUM

Resolver GRC Cloud Copyright © Resolver 2014, All rights reserved.

risk oversight solutions
A better response to risk.

5LoA: Core elements

Risk assessment rigour and independent assurance requirements defined by C-suite and the board



RiskStatusNet | Manage | Report | Administration | admin

Rebuild | Refresh | Save Snapshot | Assessor | Print | Export

Sample Summary Report for Senior Exec and The Board:

Corporate	Description	End Result Objective Owner / Sponsor(s)	Composite Residual Risk Rating (CRRR)	CRRR Update Date	Potential to Increase Entity Value	Potential to Erode Entity Value	Current Risk Assessment Rigor (RAR)	Independent Assurance Level (IAL)
	Ensure that financial statements are reliable and in compliance with GAAP.	Tim Leech	6 - Major	6/12/2014	Medium	Low	Medium (M)	LOW
	Safeguard and enhance ABC's reputation	Tim Leech	4 - Advanced	6/10/2014	High	High	Very Low (VL)	MEDIUM

Resolver GRC Cloud Copyright © Resolver 2014, All rights reserved.

risk oversight solutions
A better response to risk.

5LoA: Core elements

Requires the full range of risk treatments be identified and assessed not just “internal controls”

3.8.1 - risk treatment - process to modify **risk (1.1)**

NOTE 1 Risk treatment can involve:

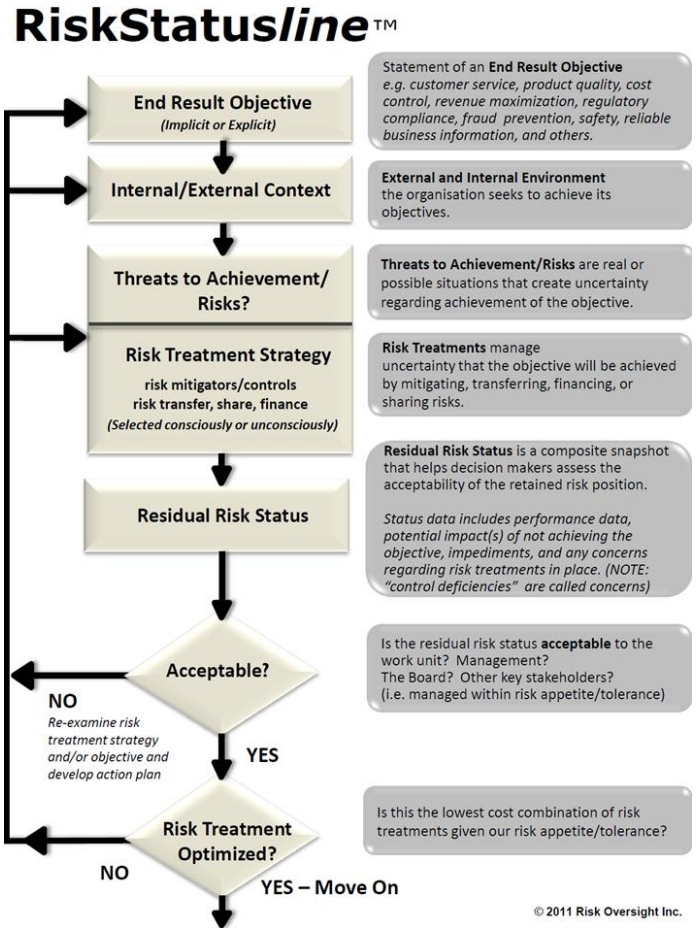
- avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
- taking or increasing risk in order to pursue an opportunity;
- removing the **risk source (3.5.1.2);**
- changing the **likelihood (3.6.1.1);**
- changing the **consequences (3.6.1.3);**
- sharing the risk with another party or parties [including contracts and **risk financing (3.8.1.4)]; and**
- retaining the risk by informed decision.

NOTE 2 Risk treatments that deal with negative consequences are sometimes referred to as “risk mitigation”, “risk elimination”, “risk prevention” and “risk reduction”.

NOTE 3 Risk treatment can create new risks or modify existing risks

5LoA: Core elements

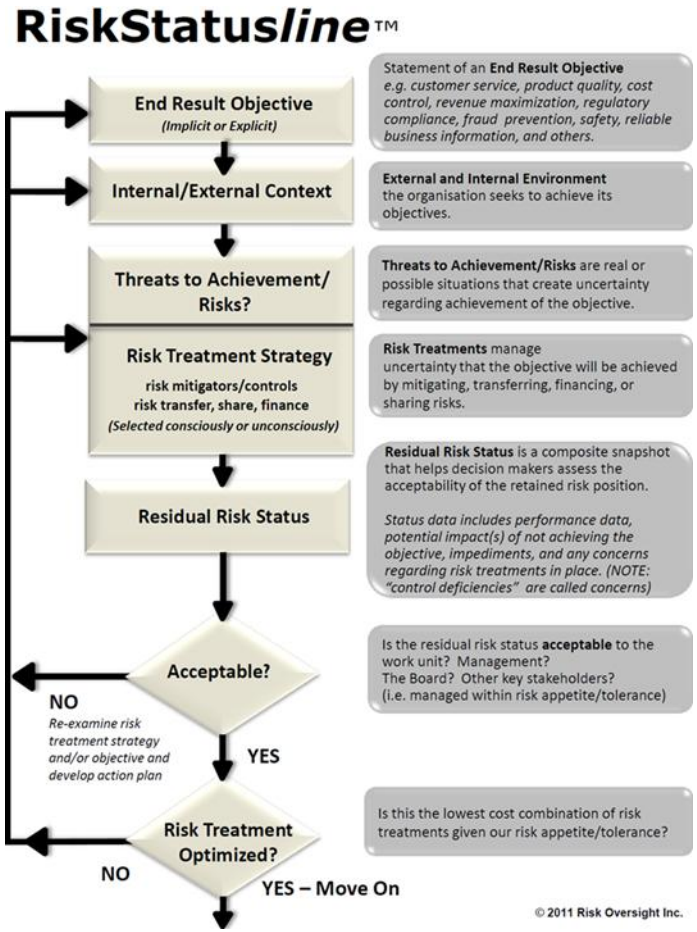
Primary focus is on the acceptability of residual risk status



risk oversight solutions
A better response to risk.

5LoA: Core elements

Specific consideration whether risk treatments are optimized



risk oversight solutions
A better response to risk.

5LoA: Key benefits

Boards are active participants not bystanders

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

Source: Financial Stabity Board Principles for Effective Risk Appetite Frameworks

5LoA: Key benefits

CEOs or their designate are responsible for a consolidated report on residual risk status linked to key value creation and potentially value erosion objectives to the board

risk oversight solutions
A better response to risk.

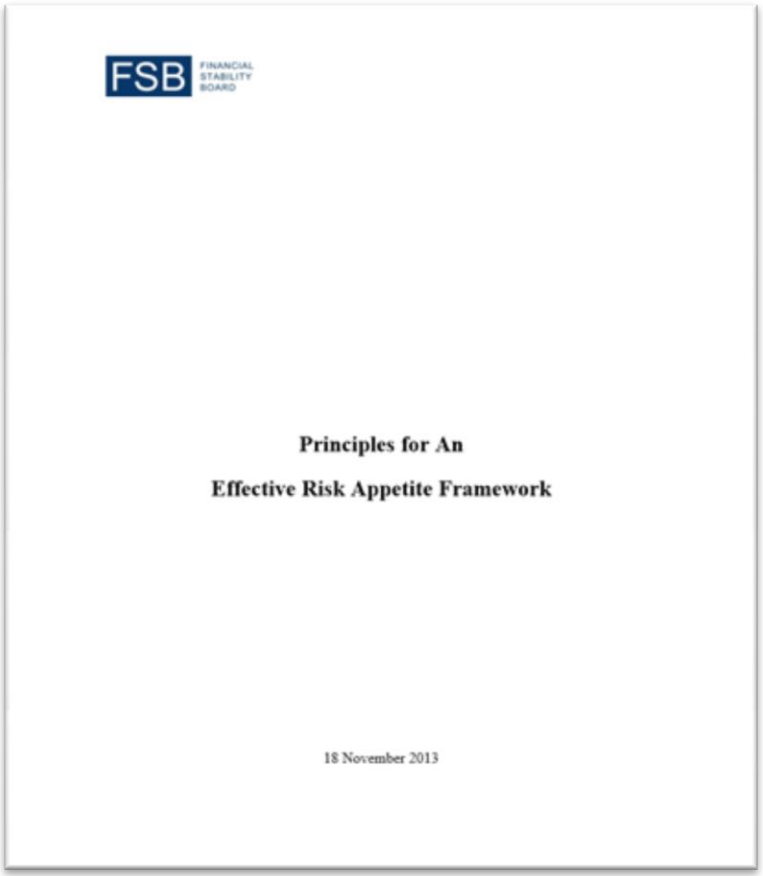
5LoA: Key benefits

Emphasis is on balancing risk taking and risk treatment

risk oversight solutions
A better response to risk.

5LoA: Key benefits

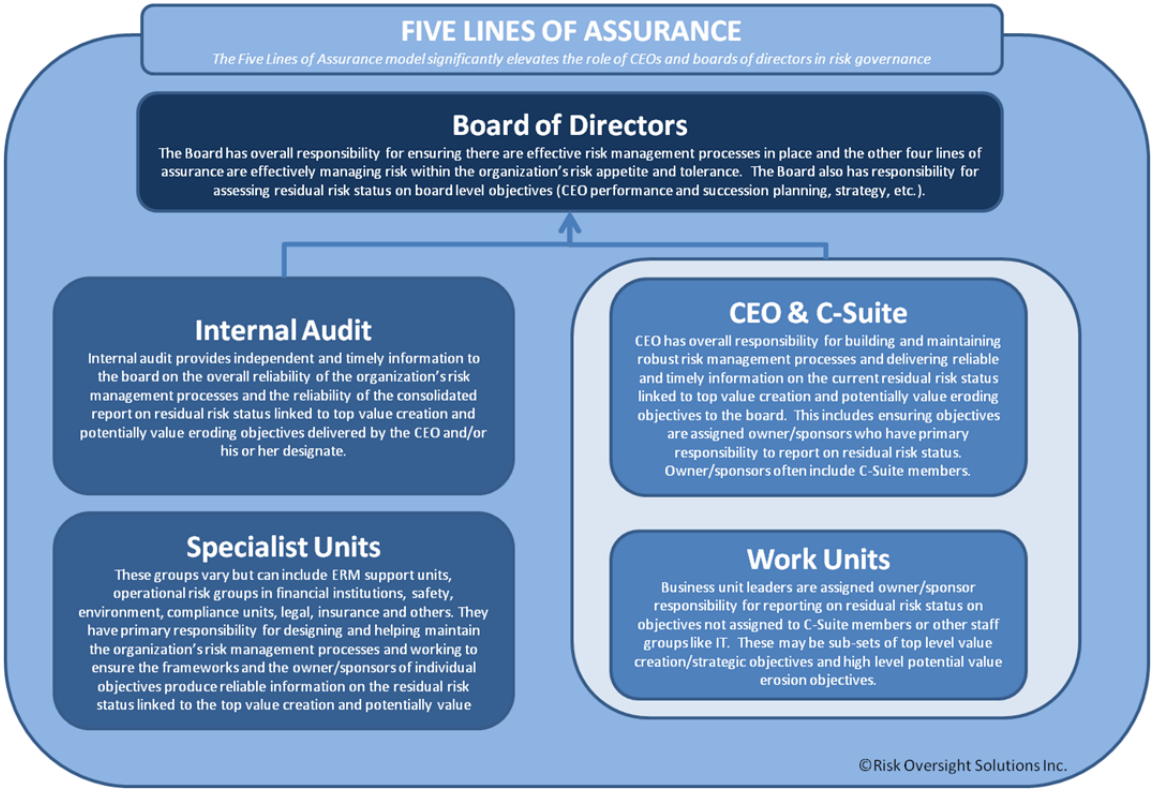
5LoA is aligned with FSB risk management guidance – best to date globally



risk oversight solutions
A better response to risk.

5LoA: Key benefits

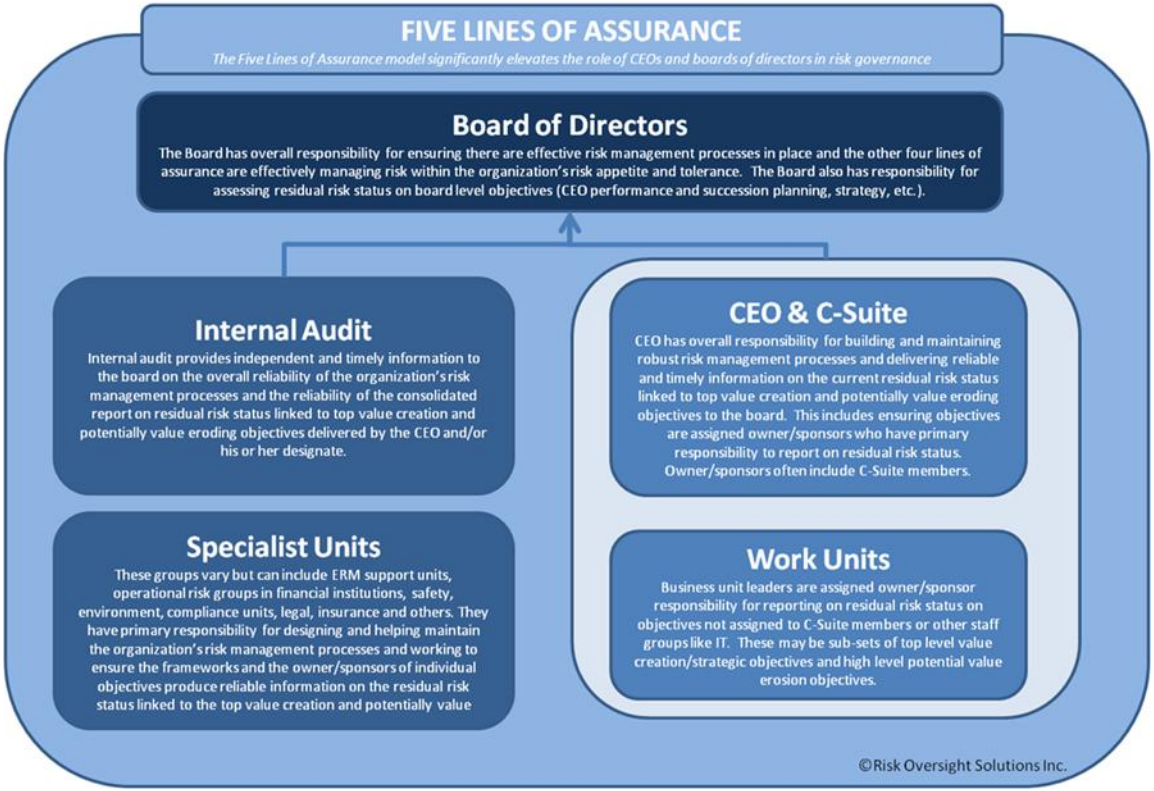
Internal audit audit's role and stature are elevated



risk oversight solutions
A better response to risk.

5LoA: Key benefits

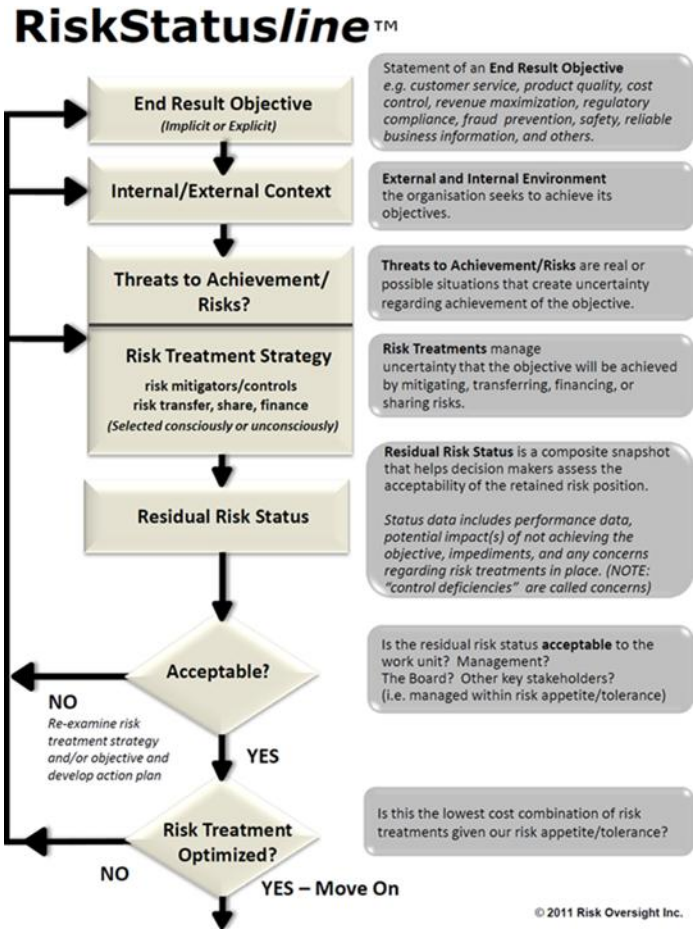
The role of specialist units is clarified



risk oversight solutions
A better response to risk.

5LoA: Key benefits

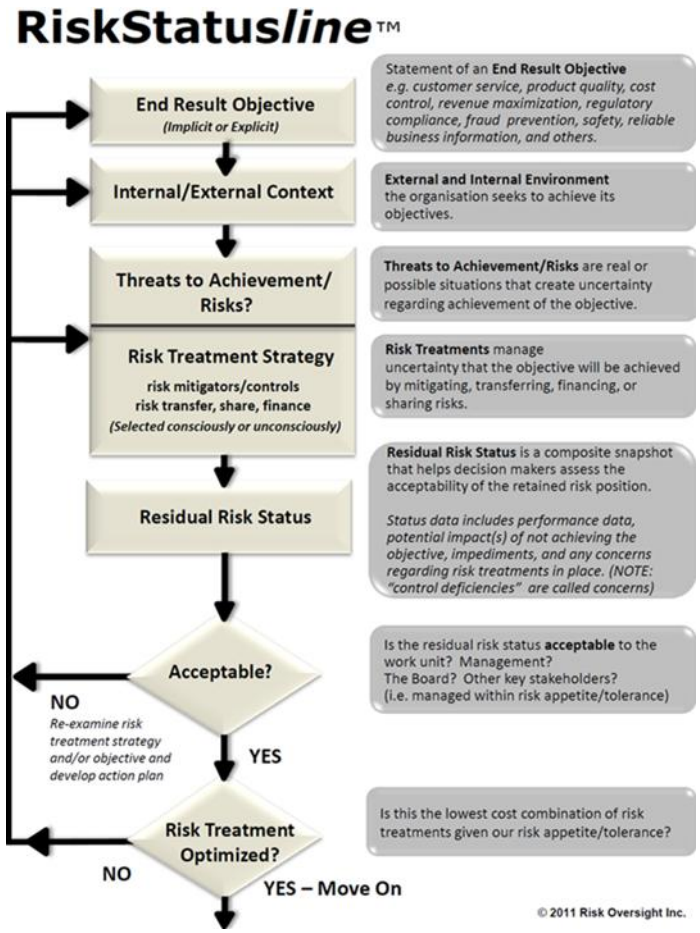
"Optimizing" risk treatments is a key goal



risk oversight solutions
A better response to risk.

5LoA: Key benefits

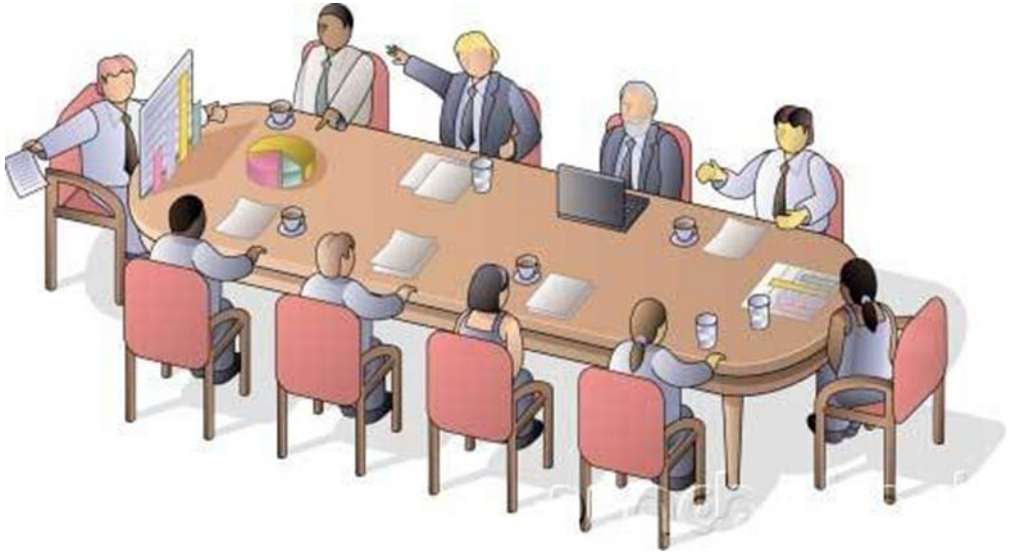
Over time the word "controls" will be replaced with "risk treatments"



risk oversight solutions
A better response to risk.

5LoA: Key benefits

Communicates and reinforces the key role CEOs and boards must/should play going forward



risk oversight solutions
A better response to risk.

5LoA: Key benefits

Supports better resource allocation decisions

5LoA: Why haven't the IIA and risk associations supported 5LoA?

Fear of change/investment in status quo

Sunk Costs

- Sunk costs
  - Costs that have been incurred as a result of past decisions
  - Unrecoverable
- Sunk-cost fallacy
  - Considering sunk costs when making new decisions at the margin
  - Can lead to using out-of-date facilities and incurring large opportunity costs

5LoA: A case study

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 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.

risk oversight solutions
A better response to risk.

5LoA: Perspectives from the Field

5LoA: Perspectives from the Field

- Risk oversight owned and actively supported by the Audit Committee of the Board of Directors. Driven and managed actively by the CFO office.
- Board support and governance – clear accountability at the Board level for oversight of risk management and active management of critical risks (CEO performance, strategy, etc.)
- 1st Phase – Aligned to the strategic plan and operating plan. Consensus on critical objectives and assigning objective owners.
- 2nd Phase – Active oversight and management of residual risk reporting related to the identified critical objectives. Define the rigor required related to each assessment.

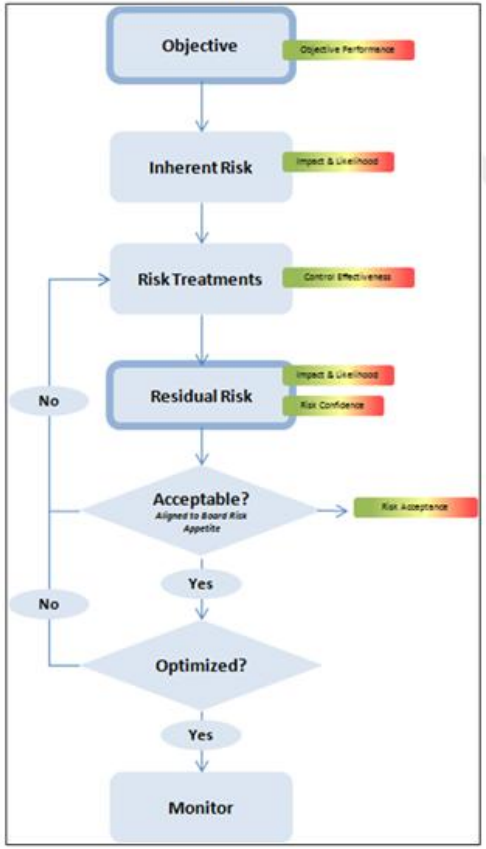
5LoA: Perspectives from the Field

Sample 1st Phase Risk Reporting Framework for Board & Methodology:

Objective-based Risk Assessment:

Division & Objective Performance	Risk	Inherent Risk	Residual Risk	Risk Mvmt Prior Q	Risk Description *(impact/likelihood, risk treatments, residual risk accept…*
Retain market share in core products of at least XY% Objective Performance: Very Positive	Risk #1			⟷	
	Risk #2			⟷	
	Risk #3			⟷	

Methodology Appendix:



risk oversight solutions
A better response to risk.

5LoA: Perspectives from the Field

Sample 1st Phase Risk Reporting Framework for Management:

Objective-Based Risk Assessment

INSTRUCTIONS:
Complete the Objective-Based Risk Assessment matrix for the key risks that could impact the defined objective. (1) Document the Objective, the Objective owner/co-sponsors, and the current Objective Performance Rating. (2) Document the key risks that could impact the achievement of the objective and provide a brief description. (3) Input the potential $ impact (could be a range) and the type of $ impact (3) Input the **inherent risk** score (impact factor, likelihood factor) and colour code the cell based on the risk matrix. (4) Document any current risk treatment factors (controls, insurance, etc.). (4) Based on the effectiveness of current mitigating factors input the **residual risk** score (impact factor, likelihood factor) and colour code the cell based on the risk matrix. (5) Input the confidence score based on available risk information. (6) Input the risk acceptance score. (7) Document any action plans that are underway or planned that could alter the residual risk score in the future.

Objective #1	**Achieve the FY## business plan targets of ## and ##**				**Objective Performance Rating**			**Positive**
Owner/ Co-Sponsor								
Key Performance Indicator Data								
#	**Risk Description**	**$**	**Inherent Risk**	**Risk Treatments**	**Residual Risk**	**Confidence**	**Acceptance**	**Action Plans**
#	***Name of risk*** [Impact & likelihood discussion including how risk treatments might alter the impact & likelihood]	$X Type $ Impact	Impact/ Likelihood	• [Control] – [Effectiveness: L, M, H] • [Insurance]	Impact/ Likelihood	H/M/L	Y/N	➢
1				•				➢
2				•				➢
3				•				➢

risk oversight solutions
A better response to risk.

5LoA: Perspectives from the Field

Common Challenges:

- Multiple divisions in locations across the globe.
- Decentralized organizational structures.
- Existing risk management processes based on traditional approaches.
- Risk management historically performed using a bottoms-up approach.
- Different levels of maturity on risk management principles and techniques.
- Ability to drive RO approach contingent on assigning ownership. If ownership difficult to establish, this is a risk in itself.

5LoA: Perspectives from the Field

Critical Success Factors:

- Buy-in from C-Suite is critical to implementation. Must be actively tied into existing strategic/operational reviews vs. being seen as a separate activity.
- Ownership of objectives assigned directly from the C-Suite.
- Not an overnight process. Rigor and confidence in the risk assessments increased over time with training and active debates and conversations on how risk data was obtained/gathered, and how risk treatment information was assessed.
- Openness to having the tough conversations on risk acceptance decisions (accept the risk vs. spending more $ (time/resources/etc.) on additional risk treatments).

5LoA: the future

risk oversight solutions
A better response to risk.

QUESTIONS???

www.riskoversightsolutions.com