risk oversight solutions

*A better response to risk.*

# Paradigm Paralysis in ERM and Internal Audit: *A Big Risk to Better Governance*

Conference Board of Canada Webinar

December 7, 2016

Tim Leech FCPA CIA CRMA CCSA CFE

**Risk Oversight Solutions Inc.**

timleech@riskoversightsolutions.com

© Risk Oversight Solutions Inc.

# Speaker Professional Profile

© Risk Oversight Solutions Inc.

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 – "Objective Centric Five Lines of Assurance". The goal – respond to the rapid escalation in board risk oversight expectations and deliver substantially more "bang for the buck" from formal assurance spending.

He has authored papers and done webinars on risk governance related topics for Conference Board in Canada, Europe and the U.S.

# Presentation Agenda

© Risk Oversight Solutions Inc.

- What is “Paradigm Paralysis”?
- Paradigm paralysis: ERM
- Paradigm paralysis: Internal Audit (IA)
- Who is most negatively impacted by ERM/IA paralysis?
- Who could drive positive change?
- Barriers to change
- The way forward: OBJECTIVE CENTRIC FIVE LINES OF ASSURANCE (OC5LoA)
- OC5LoA: The business case
- OC5LoA: Implementation options
- Questions

# What is “Paradigm Paralysis”?

© Risk Oversight Solutions Inc.

## What is paradigm paralysis? Or more basically, what is a paradigm?

*As you probably know, a paradigm is a model or a pattern. It's a shared set of assumptions that have to do with how we perceive the world.*

*Paradigms are very helpful because they allow us to develop expectations about what will probably occur based on these assumptions. But when data falls outside our paradigm, we find it hard to see and accept. This is called the PARADIGM EFFECT. And when the paradigm effect is so strong that we are prevented from actually seeing what is under our very noses, we are said to be suffering from paradigm paralysis.*

(Source:https://www.mnsu.edu/comdis/kuster/Infostuttering/Paradigmparalysis.html)

# Paradigm Paralysis: ERM Methods

© Risk Oversight Solutions Inc.

## Risk register

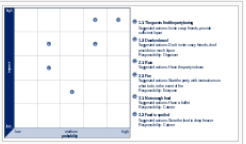
From Wikipedia, the free encyclopedia

A **risk register** (or **risk log** e.g. in PRINCE2) is a scatterplot used as risk management tool and to fulfill regulatory compliance acting as a repository for all risks identified and includes additional information about each risk, e.g. nature of the risk, reference and owner, mitigation measures.

ISO 73:2009 Risk management—Vocabulary[1] defines a risk register to be a "record of information about identified risks".

Contents [hide]





A **Risk register** plots the impact of a given risk over of its probability. The presented example deals with some issues which can arise on a usual Saturday-night party.

### Example [ edit ]

Risk register the project "barbecue party" with somebody inexperienced handling the grill, both in table format (below) and as plot (right).

| Category | Name | - | Probability | Impact | Mitigation | Contingency | Risk Score after Mitigation | Action By | Action When |
|---|---|---|---|---|---|---|---|---|---|
| Guests | The guests find the party boring | 1.1. | low | medium | Invite crazy friends, provide sufficient liquor | Bring out the karaoke | 2 | | within 2hrs |
| Guests | Drunken brawl | 1.2. | medium | low | Don't invite crazy friends, don't provide too much liquor | Call 911 | x | | Now |
| Nature | Rain | 2.1. | low | high | Have the party indoors | Move the party indoors | 0 | | 10mins |
| Nature | Fire | 2.2. | highest | highest | Start the party with instructions on what to do in the event of fire | Implement the appropriate response plan | 1 | Everyone | As per plan |
| Food | Not enough food | 3.1. | high | high | Have a buffet | Order pizza | 1 | | 30mins |
| Food | Food is spoiled | 3.2. | high | highest | Store the food in deep freezer | Order pizza | 1 | | 30mins |

### Terminology [ edit ]

A Risk Register can contain many different items. There are recommendations for Risk Register content made by the Project Management Institute Body of Knowledge (PMBOK) and PRINCE2. ISO 31000:2009[3] does not use the term risk register, however it does state that risks need to be documented.

There are many different tools that can act as risk registers from comprehensive software suites to simple spreadsheets. The effectiveness of these tools depends on their implementation and the organisation's culture.[*citation needed*]

A typical risk register contains:

- A risk category to group similar risks

An example of the Risk Register for a project that includes 4 steps: Identify, Analyze, Plan Response, Monitor and Control. [2]

risk oversight solutions
*A better response to risk.*

# Paradigm Paralysis: ERM Methods

© Risk Oversight Solutions Inc.


risk oversight solutions
*A better response to risk.*

# Paradigm Paralysis: ERM Methods

© Risk Oversight Solutions Inc.

**What's wrong with the COSO June 2016 ERM exposure draft?**

- LACK OF RESEARCH ON CAUSES OF ERM FAILURES
- STRADDLING TWO CONFLICTING ERM PARADIGMS
- CONFLICTING GUIDANCE ON ERM AND INTERNAL CONTROL
- LACK OF RECOGNITION AND INTEGRATION WITH ISO 31000 RISK MANAGEMENT STANDARD
- THE ROLE OF INTERNAL AUDIT

Source:http://erm.coso.org/Uploads/Tim_Leech_Risk_Oversight_Solutions_Inc._ERM_Exposure_9-7-2016.pdf

# Paradigm Paralysis: Internal Audit

© Risk Oversight Solutions Inc.

## Internal audit

From Wikipedia, the free encyclopedia

**Internal auditing** is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.[1] Internal auditing is a catalyst for improving an organization's governance, risk management and management controls by providing insight and recommendations based on analyses and assessments of data and business processes.[2] With commitment to integrity and accountability, internal auditing provides value to governing bodies and senior management as an objective source of independent advice. Professionals called internal auditors are employed by organizations to perform the internal auditing activity.

The scope of internal auditing within an organization is broad and may involve topics such as an organization's governance, risk management and management controls over: efficiency/effectiveness of operations (including safeguarding of assets), the reliability of financial and management reporting,[3][4] and compliance with laws and regulations. Internal auditing may also involve conducting proactive fraud audits to identify potentially fraudulent acts; participating in fraud investigations under the direction of fraud investigation professionals, and conducting post investigation fraud audits to identify control breakdowns and establish financial loss.

Internal auditors are not responsible for the execution of company activities; they advise management and the Board of Directors (or similar oversight body) regarding how to better execute their responsibilities. As a result of their broad scope of involvement, internal auditors may have a variety of higher educational and professional backgrounds.

# Paradigm Paralysis: Internal Audit

## Key Attributes of Traditional "Direct Report" Internal Audit

© Risk Oversight Solutions Inc.

- Internal audit creates and maintain a "audit universe" – units/topics/things IA believes it could "audit"
- IA complete audits of audit universe elements selected for the year and provide an opinion whether they think "internal controls" in the area examined are "effective" or "deficient".
- This traditional IA approach is called "direct report" auditing. The person responsible for the area being audited does not make a representation on the state of risk/control/residual risk. If they did, and IA completed an audit of the representation from the responsible person(s), it would be called a "attestation" audit. Financial statement audits done by external auditors are attestation audits. Auditors opine on whether it is reliable, not whether they like it or think it's not "effective".

# Paradigm Paralysis: Internal Audit

© Risk Oversight Solutions Inc.

## Key Attributes of Traditional "Direct Report" Internal Audit

- Annual coverage is usually less than 5% of the total risk universe
- Coverage frequently does not include the organization's top value creation objectives (objectives key to the long term success of the enterprise that will create enhanced stakeholder value)
- History indicates the traditional IA approach frequently misses major risks to the organization's long term success
- Auditees frequently experience pressure to "fix" areas where IA believe internal controls are "ineffective" and relations can be adversarial
- The process can result in sub-optimal entity level resource allocation (i.e. resources are directed to fix areas identified as "deficient" by IA because of board pressure not because they are where resources are most needed)

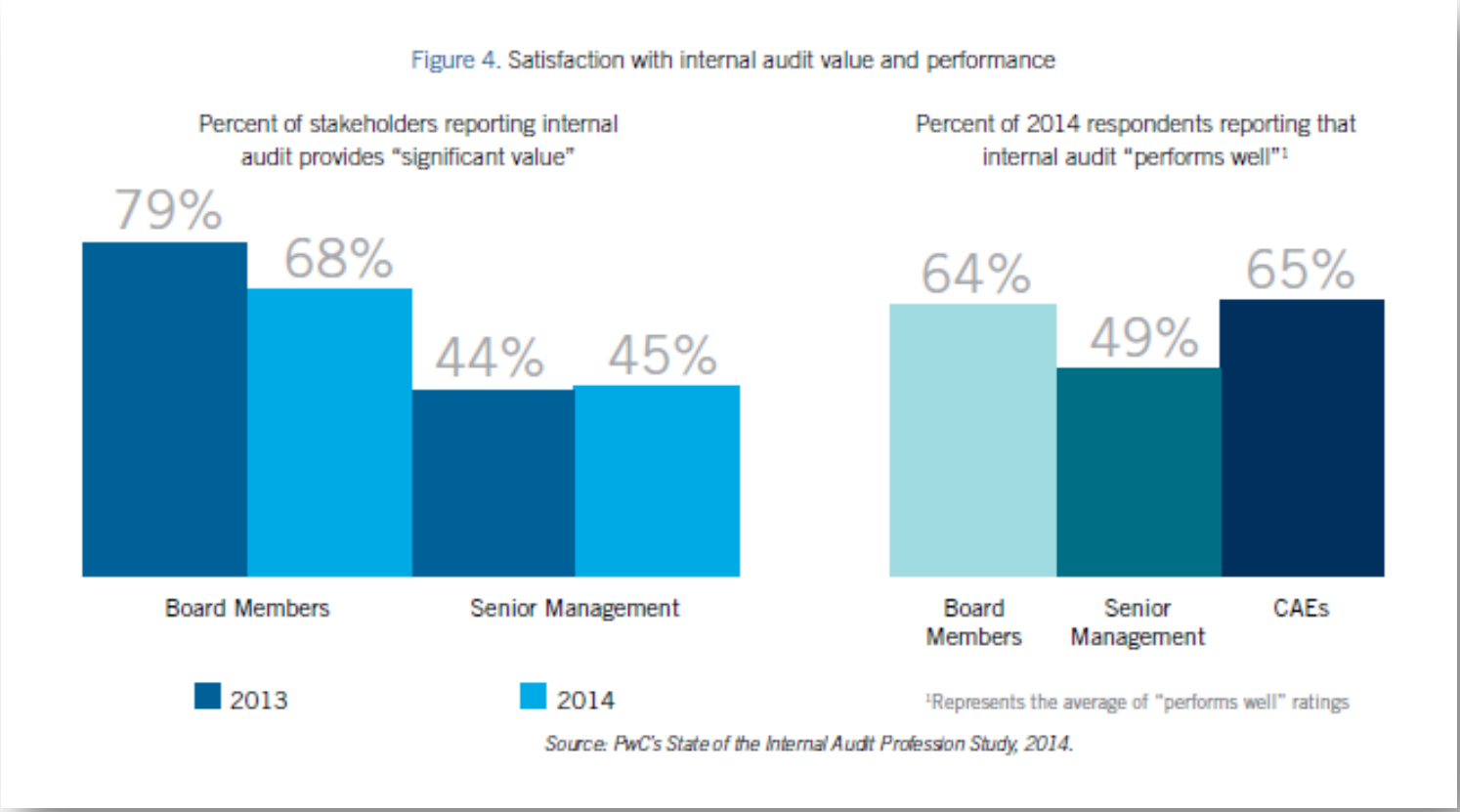
# Who is most negatively impacted by ERM/IA paradigm paralysis?

© Risk Oversight Solutions Inc.

## Those impacted by major governance failures

# Who is most negatively impacted by ERM/IA paradigm paralysis?

© Risk Oversight Solutions Inc.




risk oversight solutions
*A better response to risk.*

# Who is most negatively impacted by ERM/IA paradigm paralysis?

© Risk Oversight Solutions Inc.

## Global State of Enterprise Risk Oversight: 2nd Edition

- **60%** of boards of directors in most regions of the world are placing significant pressure on organisations to increase senior management's involvement in risk oversight.
- **70%** or more of boards in all regions of the world outside the U.S. are formally assigning risk oversights responsibilities to a board committee. Surprisingly, only 46% of U.S. boards are doing so
- Less than half (**42%**) of organisations discuss risk information generated by the ERM process when the board discusses the organisation's strategic plan.
- Over **60%** of organisations in most regions have internal management level risk committees. The exception is in the U.S, where only 44% indicate they have those committees in place.
- Few organisations (around **20%**) integrate risk management activities with performance compensation/remuneration and most (about **80%**) have not invested in risk management training for executives in the past few years.

Source: http://www.cgma.org/Resources/Reports/DownloadableDocuments/2015-06-13-The-global-state-of-enterprise-risk-oversight-report.pdf

# Who is most negatively impacted by ERM/IA paradigm paralysis?

© Risk Oversight Solutions Inc.

## Global State of Enterprise Risk Oversight: 2nd Edition

- About **60%** of organisations worldwide agree that they face a wide array of complex and increasing risk issues.
- Despite that, **35%** or fewer organisations claim to have formal enterprise risk management in place.
- About **70%** of organisations would not describe their risk management oversight as mature.
- **40%** or fewer organisations are satisfied with the reporting of information about top risk exposures to senior management.
- Less than **30%** view their risk management process as providing competitive advantage.

Source: http://www.cgma.org/Resources/Reports/DownloadableDocuments/2015-06-13-The-global-state-of-enterprise-risk-oversight-report.pdf

# Who could drive positive change?

© Risk Oversight Solutions Inc.


OSFI
BSIF

U.S. SECURITIES AND EXCHANGE COMMISSION
MCMXXXIV

risk oversight solutions
*A better response to risk.*

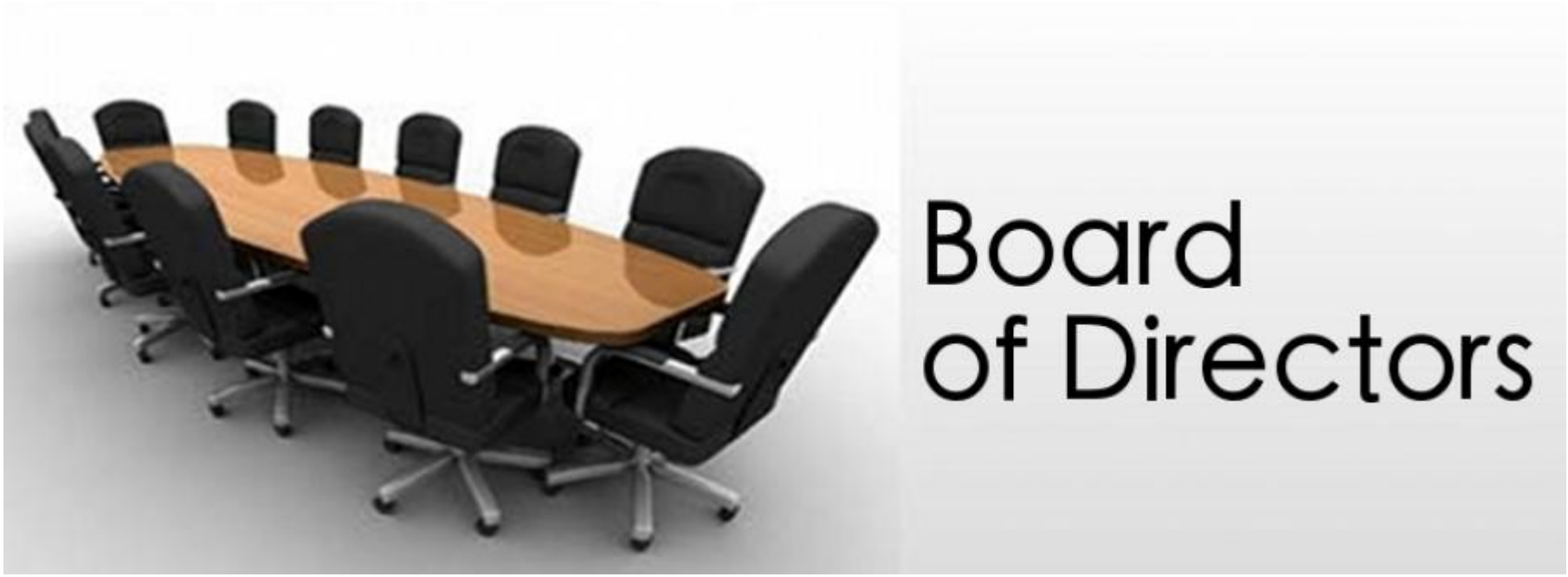
# Who could drive positive change?

© Risk Oversight Solutions Inc.


risk oversight solutions
*A better response to risk.*

# Who could drive positive change?

© Risk Oversight Solutions Inc.




risk oversight solutions
*A better response to risk.*

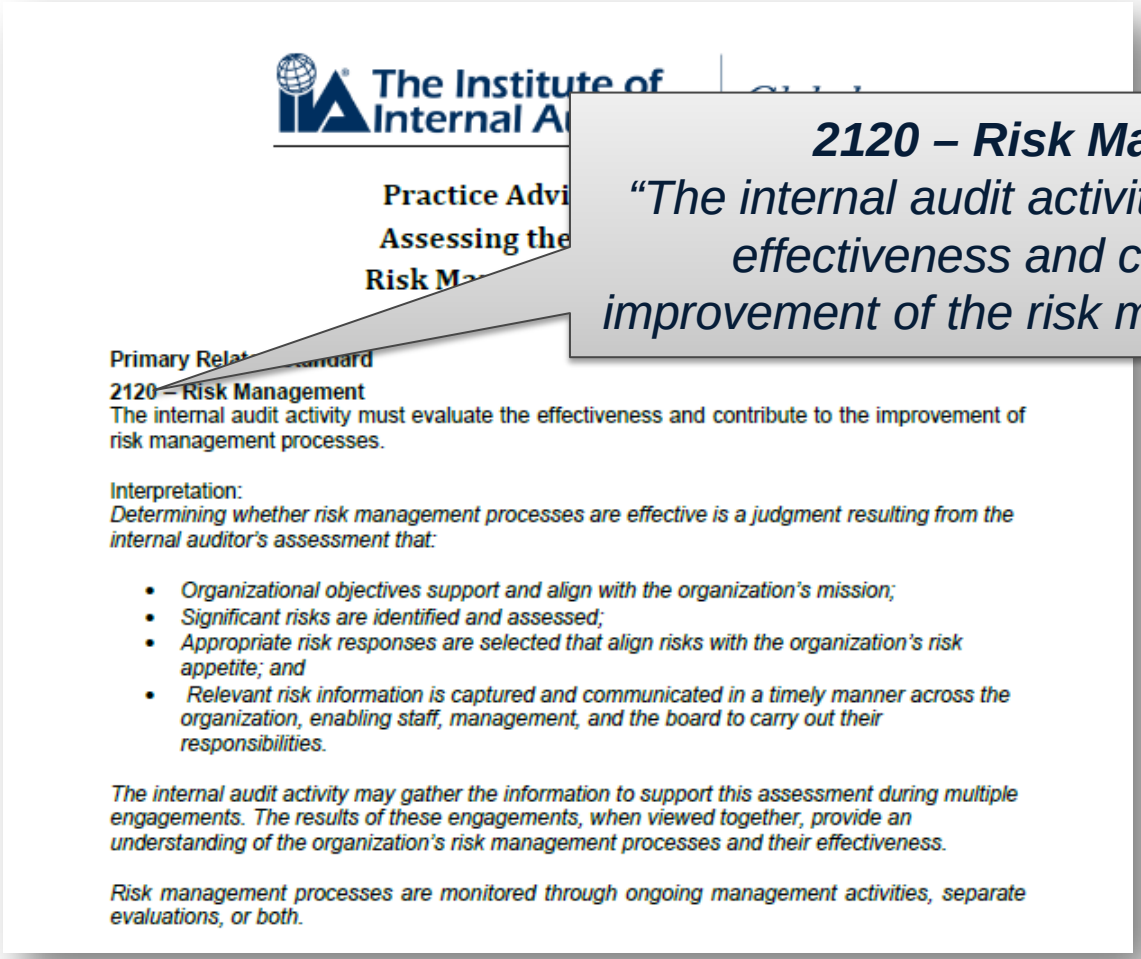
# Who could drive positive change?

© Risk Oversight Solutions Inc.

risk oversight solutions
*A better response to risk.*

# Who could drive positive change?

© Risk Oversight Solutions Inc.



The Institute of Internal A

Practice Advi
Assessing the
Risk Ma

Primary Relat standard

**2120 – Risk Management**
The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

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

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

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

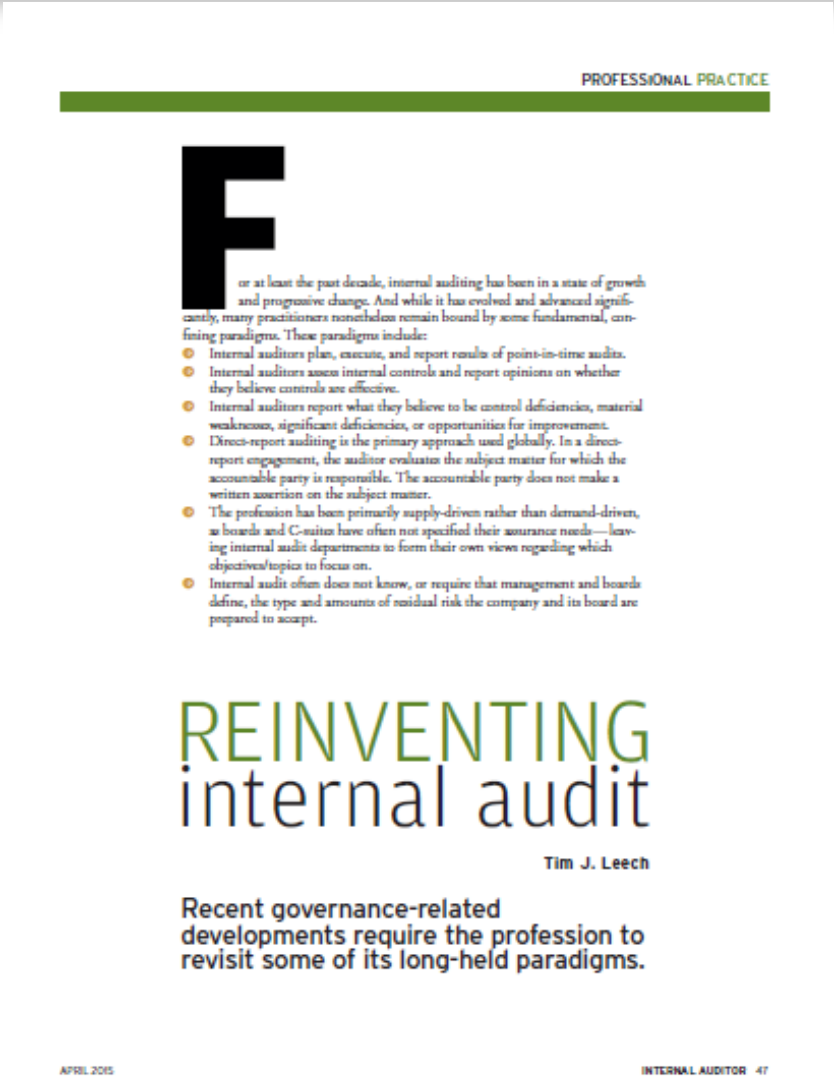
*Risk management processes are monitored through ongoing management activities, separate evaluations, or both.*

***2120 – Risk Management***
*"The internal audit activity must evaluate the effectiveness and contribute to the improvement of the risk management process"*

risk oversight solutions
*A better response to risk.*

# Who could drive positive change?

© Risk Oversight Solutions Inc.



PROFESSIONAL PRACTICE

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 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-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-suites 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.

## REINVENTING internal audit

Tim J. Leech

**Recent governance-related developments require the profession to revisit some of its long-held paradigms.**

APRIL 2015 INTERNAL AUDITOR 47

risk oversight solutions
*A better response to risk.*

# Who could drive positive change?

© Risk Oversight Solutions Inc.


risk oversight solutions
*A better response to risk.*

# Who could drive positive change?

© Risk Oversight Solutions Inc.

# Barriers to change

© Risk Oversight Solutions Inc.

**Barriers to Paradigm Shifts**

**The greatest barrier to a paradigm shift is the reality and incredible inertia of paradigm paralysis. A paradigm paralysis can be defined as the inability or refusal to see beyond current models of thinking. There are countless examples of paradigm paralysis in the history of mankind. In Europe, up until the XVII century, physicians used to draw out substantial amount of blood from their patients to "purify" their bodies from some imaginary "miasma". It would, of course, make patients weaker and quicken their death. The first physicians to challenge this absurdity were dismissed and banned from the profession. A better known example of paradigm paralysis is the rejection of Galileo's theory of a heliocentric universe which revolutionized the field of astronomy.**

**Source: http://newsjunkiepost.com/2011/09/04/will-we-have-a-global-paradigm-shift-away-from-obsolete-ideologies/**

# Barriers to change

© Risk Oversight Solutions Inc.

## Regulator paradigm paralysis

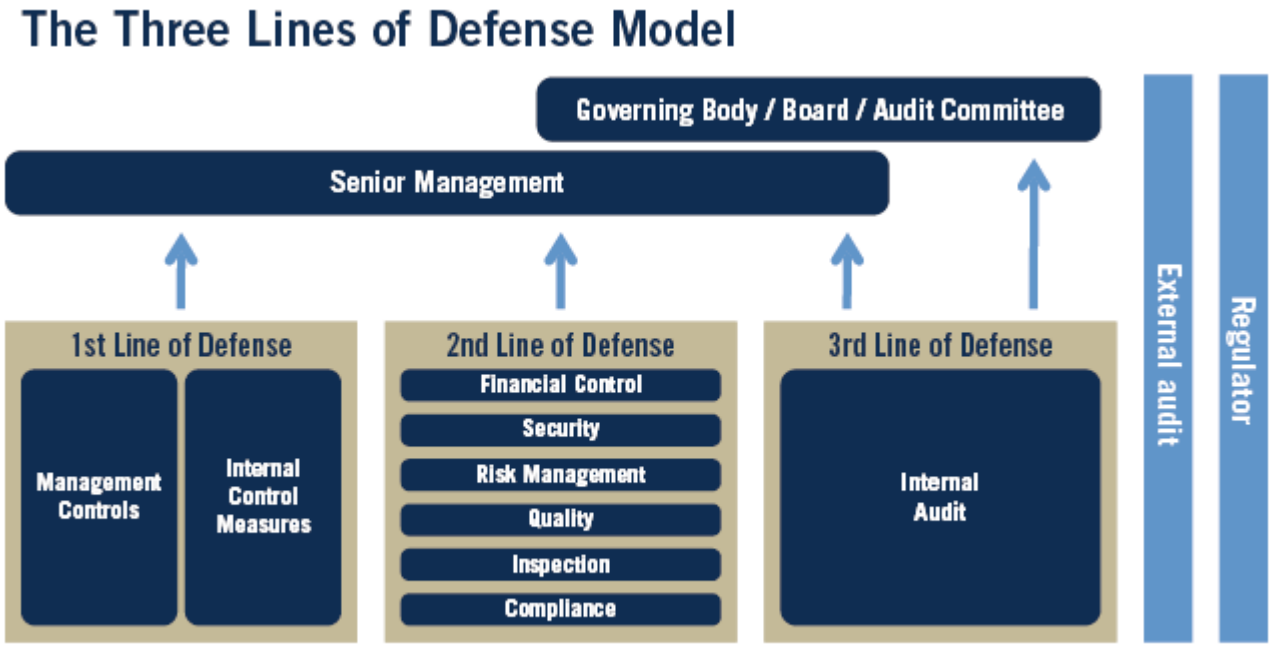

# Barriers to change

© Risk Oversight Solutions Inc.


risk oversight solutions
*A better response to risk.*

# Barriers to change

© Risk Oversight Solutions Inc.




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

risk oversight solutions
*A better response to risk.*

# Barriers to change

© Risk Oversight Solutions Inc.

## 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

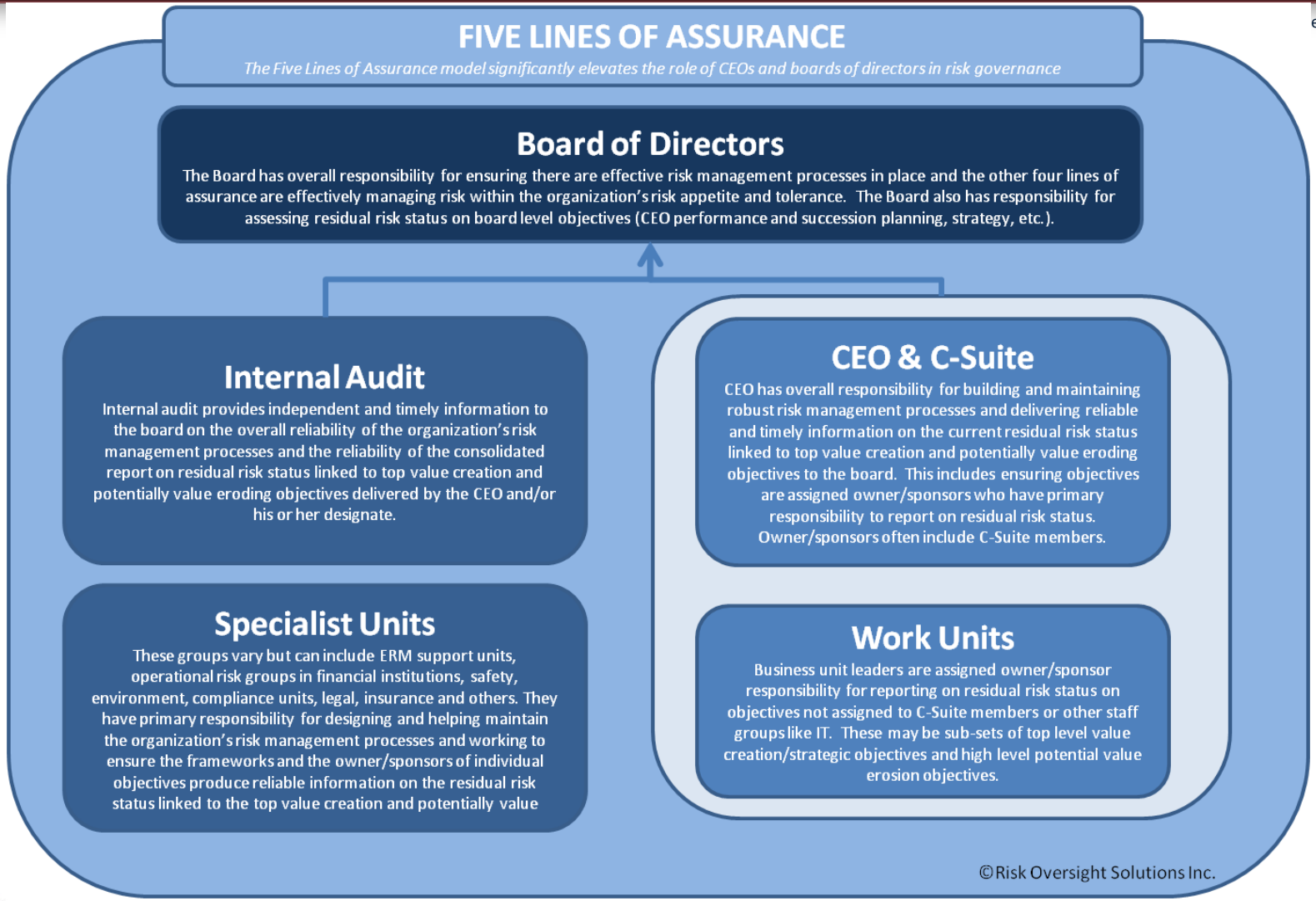
- For most organizations with a risk management committee, the committee meets at least quarterly.

*Source: http://www.aicpa.org/interestareas/businessindustryandgovernment/resources/erm/downloadabledocuments/aicpa_erm_research_study_2015.pdf*

risk oversight solutions
*A better response to risk.*

# The Way Forward: Objective Centric 5LoA

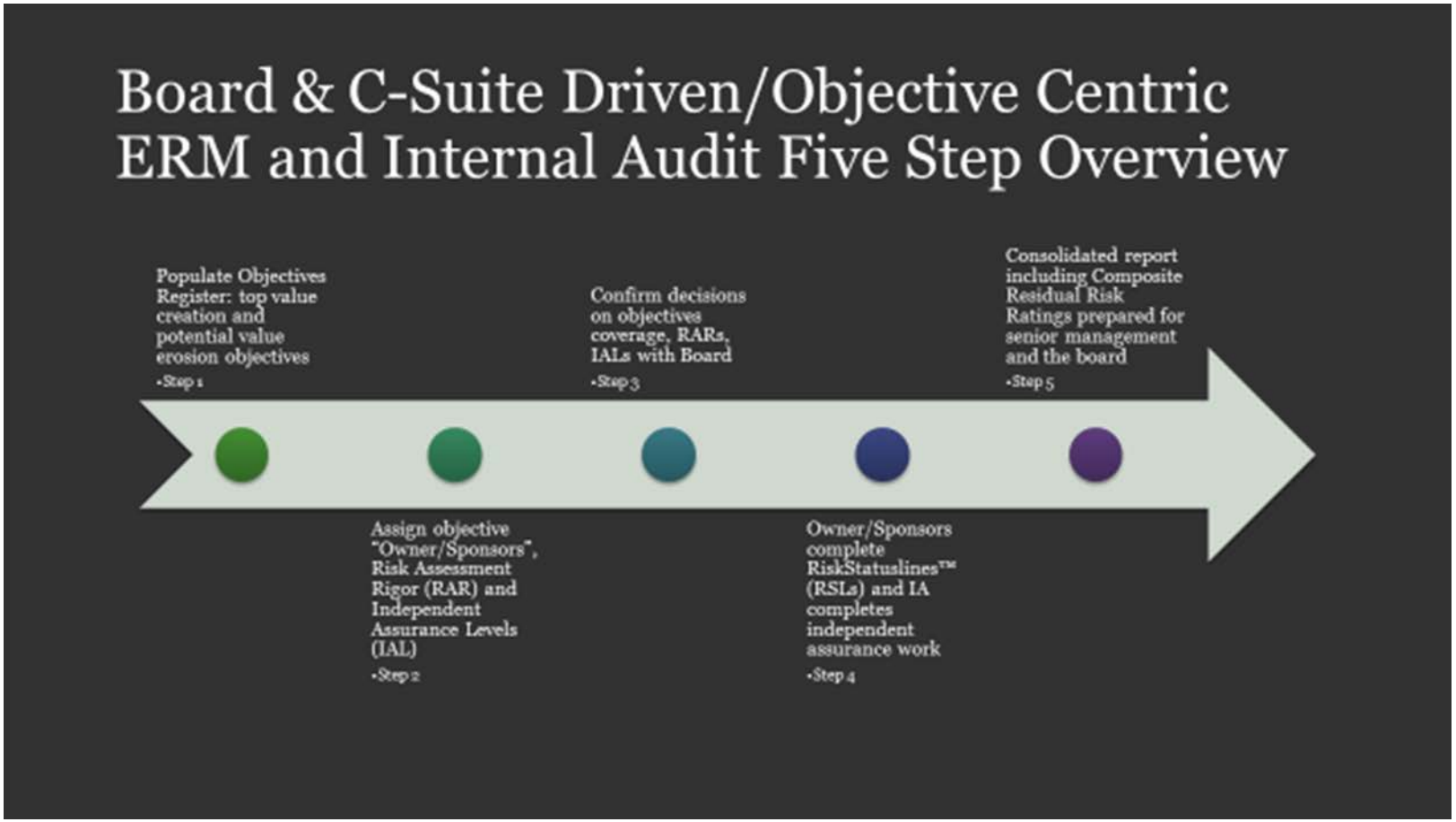
ersight Solutions Inc.




risk oversight solutions
*A better response to risk.*

# The Way Forward: Objective Centric 5LoA

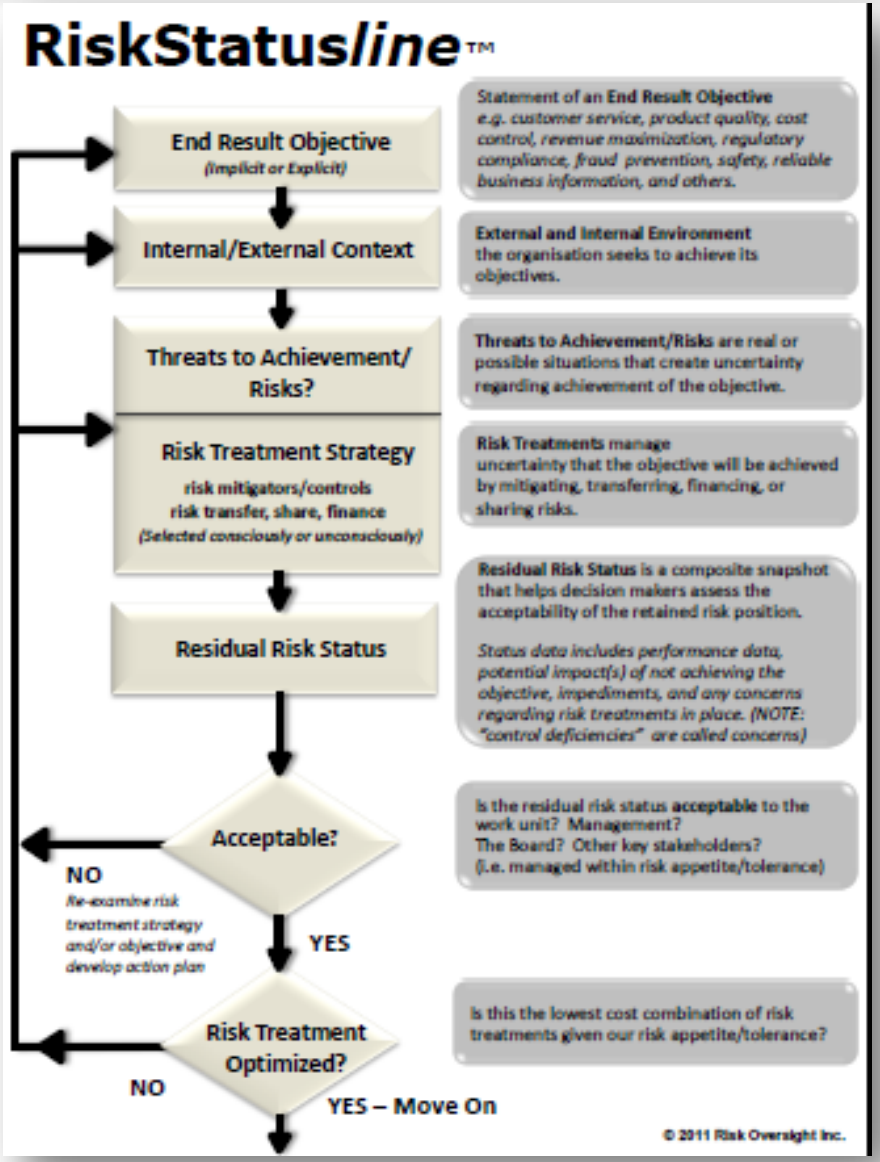
© Risk Oversight Solutions Inc.




risk oversight solutions
*A better response to risk.*

# The Way Forward: Objective Centric 5LoA

© Risk Oversight Solutions Inc.

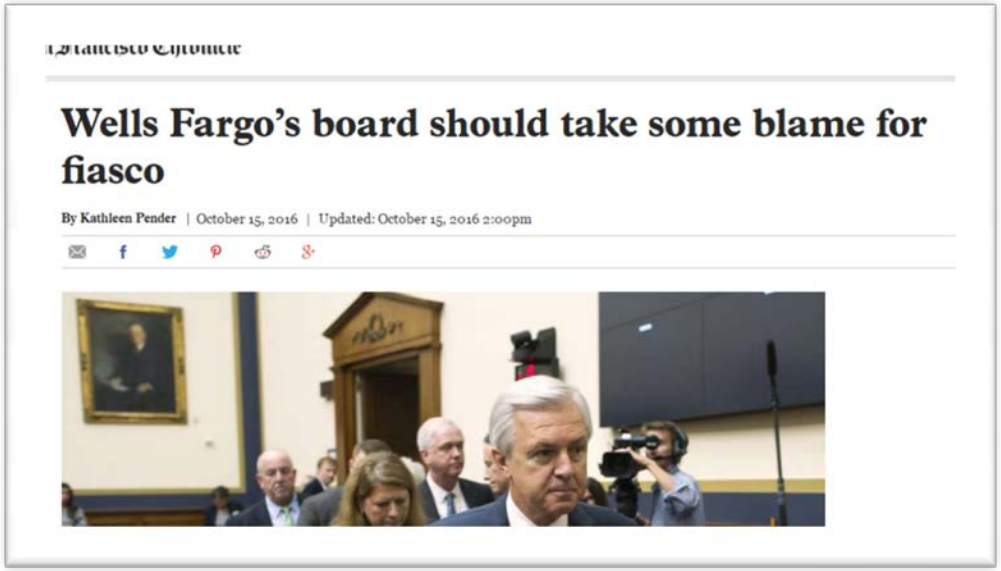



risk oversight solutions
*A better response to risk.*

# OC5LoA: the business case

© Risk Oversight Solutions Inc.

- Boards are active participants, not bystanders.
- Communicates and reinforces the key role the CEO and the Board must/should play in ERM going forward.



San Francisco Chronicle

**Wells Fargo's board should take some blame for fiasco**

By Kathleen Pender | October 15, 2016 | Updated: October 15, 2016 2:00pm



Twitter Shareholder Sues CEO and Board Members Over Inflated Share Price

by Jeff John Roberts @jeffjohnroberts OCTOBER 26, 2016, 9:50 AM EDT



risk oversight solutions
*A better response to risk.*

# OC5LoA: the business case

© Risk Oversight Solutions Inc.

- Emphasis is on risk taking and risk treatment
- Senior management and boards are provided with a concise picture of the state of residual risk status linked to the organization's top value creation and erosion objectives to help them assess its acceptability

# OC5LoA: the business case

© Risk Oversight Solutions Inc.

- 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
- Supports better resource allocation decisions

ro oversight solutions
*A better response to risk.*

# OC5LoA: the business case

© Risk Oversight Solutions Inc.

- The objective is not to minimize risk but rather to optimize the level of risk being accepted to best achieve the organization's objectives while still operating within an acceptable level of retained/residual risk.
- In addition to analyzing "residual risk status" the process focuses on "optimizing risk treatments" – i.e. the lowest possible cost combination of risk treatments necessary to operate within risk appetite/tolerance

# OC5LoA: the business case

© Risk Oversight Solutions Inc.

- IA focuses on the top value creation and potential value erosion objectives elevating IA's stature and value add.
- IA staff must learn to consider and assess the full range of "risk treatments" not just "internal controls".

# OC5LoA: the business case

© Risk Oversight Solutions Inc.

- 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, a common problem in direct report internal audit,  is reduced significantly

# OC5LoA: the business case

© Risk Oversight Solutions Inc.

- 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

# OC5LoA: the business case

© Risk Oversight Solutions Inc.

- Elevates ERM from what many see as a compliance activity done annually to a key part of strategy development, value creation and better managing potentially value eroding objectives.


risk oversight solutions
*A better response to risk.*

# OC5LoA: the business case

© Risk Oversight Solutions Inc.

- The role of ERM support groups is clear – Key role #1 - assist OWNER/SPONSORS of top value creation and potentially value eroding objectives to assess and report on the state of residual risk status to senior management and the board

- The role of ERM support groups is clear – Key role #2 – help OWNER/SPONSORS optimize the risk treatment design (i.e. the lowest cost possible risk treatment design capable of producing an acceptable level of residual risk

# OC5LoA:the business case

© Risk Oversight Solutions Inc.

- ERM work better supports the new expectation that boards are responsible for ensuring that effective risk management processes are in place and management is operating the organization within the board's risk appetite and tolerance

- The OC5LoA risk assessment methodology is consistent with ISO 31000 terminology/methodology and provides a solid foundation to meet the principles defined by the Financial Stability Board in their "Principles for an Effective Risk Appetite Framework

- ERM support staff receive clear instructions from senior management and the board on the level of risk assessment rigor and independent assurance they want on all objectives in the OBJECTIVES REGISTER

# OC5LoA:the business case

## 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).

SVG Capital plc
London Stock Exchange
Jan 2015 Annual Report
Page 29

© Risk Oversight Solutions Inc.

The Companies Act and FRC require companies to disclose the principal risks and uncertainties the Company faces. The Company believes this process is best done by considering the Company's most important value creation objectives and objectives that have the potential, if not achieved, to significantly erode shareholder value. Independent expert advice has been obtained to ensure that the processes used to populate and maintain the Company's objectives register and the related residual risk status information are robust, effective, and 'fit for purpose'.

'Principal risks and uncertainties' are defined by the Board as risks with the highest overall potential to affect the achievement of the Company's business objectives. These objectives include: ensuring the ability to meet liabilities as they fall due and meet liabilities in full; and achieving target returns. Principal risks relating to delivery of these objectives are described on page 30, along with other principal risks identified in relation to other key objectives. Further information on risk factors is set out in note 29 to the Accounts.

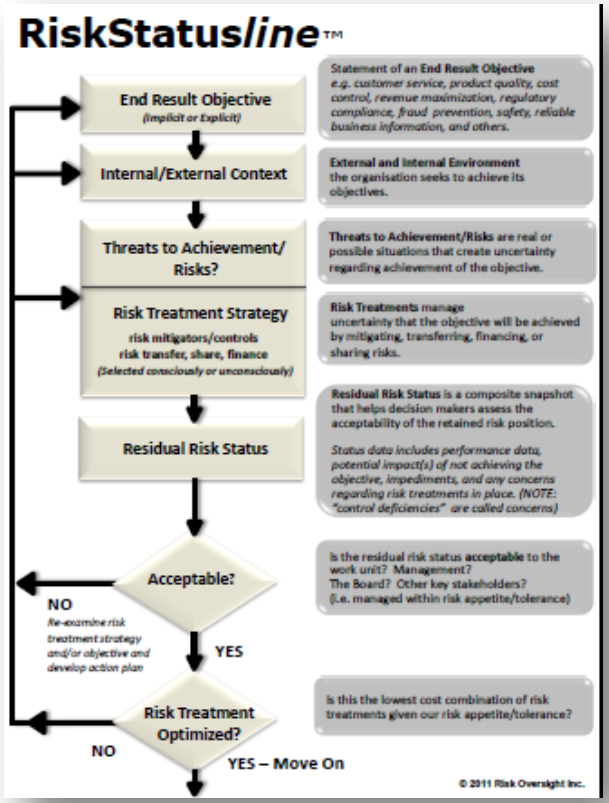
### Internal control/risk treatment

The Code requires the Board to at least annually conduct a review of the adequacy of the Company's

# OC5LoA implementation options

© Risk Oversight Solutions Inc.

## Go Slow Approach #1 – start by doing some audits using RiskStatusline™ method

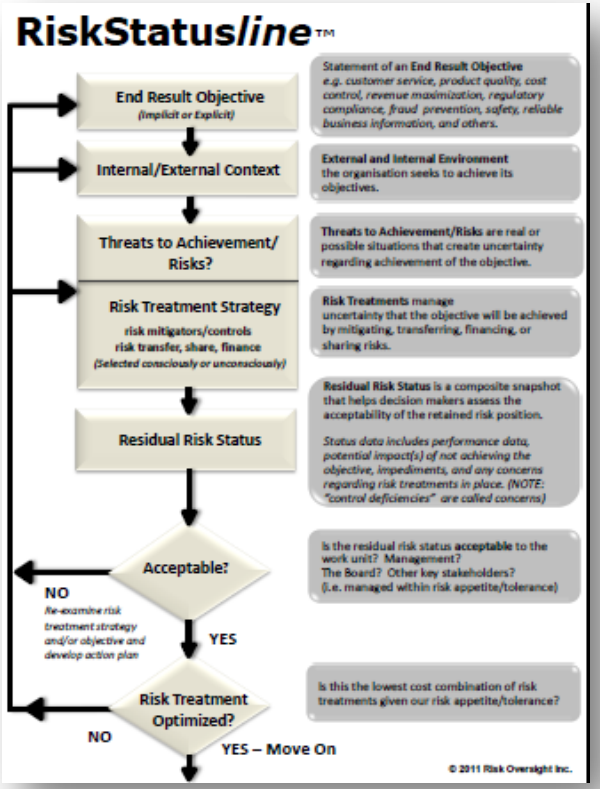



risk oversight solutions
*A better response to risk.*

# OC5LoA implementation options

© Risk Oversight Solutions Inc.

## Go Slow Approach #2 – run some risk workshops using RiskStatusline™ method

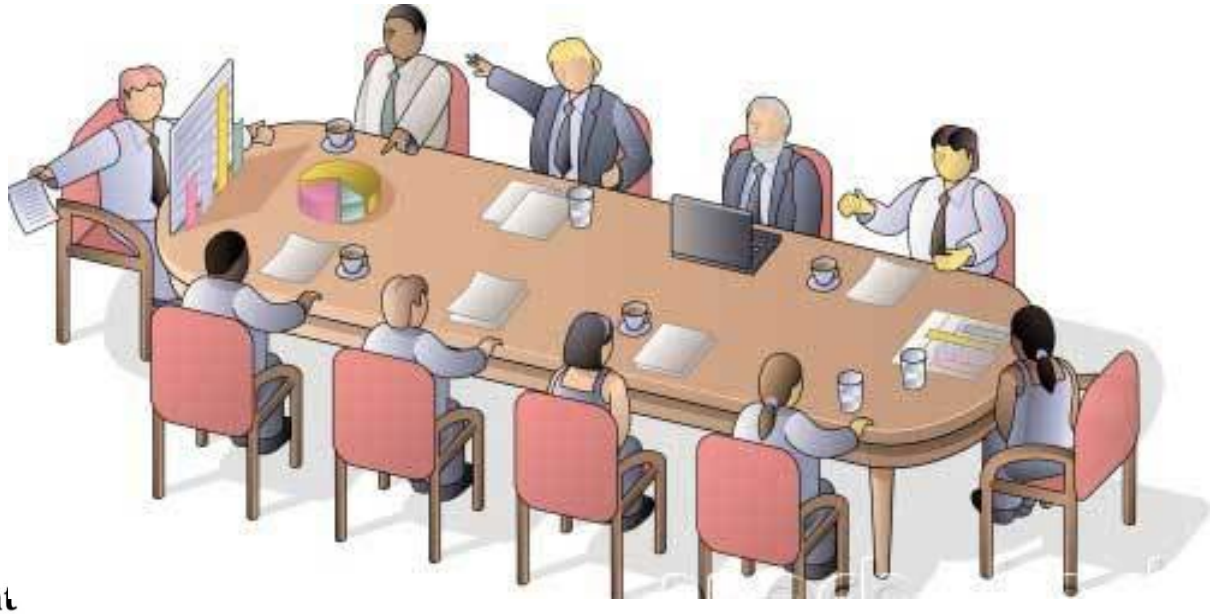



risk oversight solutions
A better response to risk.

# OC5LoA implementation options

© Risk Oversight Solutions Inc.

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



# OC5LoA implementation options

© Risk Oversight Solutions Inc.

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"


risk oversight solutions
*A better response to risk.*

© Risk Oversight Solutions Inc.

# QUESTIONS???
# Thank you

timleech@riskoversightsolutions.com

risk oversight solutions
*A better response to risk.*