

Honorably Retire “Internal Controls” Promote “Risk Treatments”: It’s Time

Tim J. Leech FCA CIA CRMA
Risk Oversight Inc.
tim.leech@riskoversight.ca

Session Overview

- Evolution of “internal control”
- Evolution of “risk treatments”
- “Risk treatment optimization” – a major opportunity to add significantly more value
- Business case for radical change
- The way forward
- Questions

Evolution of “internal control”

An example of a traditional definition

Systematic measures (such as reviews, checks and balances, methods and procedures) instituted by an organization to (1) conduct its business in an orderly and efficient manner, (2) safeguard its assets and resources, (3) deter and detect errors, fraud, and theft, (4) ensure accuracy and completeness of its accounting data, (5) produce reliable and timely financial and management information, and (6) ensure adherence to its policies and plans.

(Source: <http://www.businessdictionary.com/definition/internal-control.html>)

Evolution of “internal control”

COSO 1991 Exposure Draft – A Great Piece of Work

Internal Control is the process by which an entity’s board of directors, management and/or other personnel obtain reasonable assurance as to achievement of specified objectives; it consists of nine interrelated components, with integrity, ethical values and competence, and the control environment, serving as the foundation for the other components, which are: establishing objectives, risk assessment, information systems, control procedures, communication, managing change, and monitoring.

(Source: Internal Control - Integrated Framework Exposure Draft March 1991, Committee of Sponsoring Organizations)

Evolution of “internal control”

COSO 1992 – Final Definition – A quantum step backwards in time and thinking

Internal control is a process, effected by an entity’s board of directors, management and other personnel, designated to provide reasonable assurance regarding the achievement of objectives in the following categories:

- *Effectiveness and efficiency of operations.*
- *Reliability of financial reporting.*
- *Compliance with applicable laws and regulations.*

NOTE: In 2011 the COSO board chair concluded the 1992 definition of internal control was “timeless” and there was no need to re-examine or modify it in the COSO framework update planned for 2012. The update is now scheduled for release sometime in 2013 as a result of a groundswell of concerns and objections expressed by respondents to the 2011 exposure draft.

Evolution of “internal control”

Example: PCAOB Auditing Standard #5 for SOX 404 (b)

- 949 instances of the word “control”
- 193 instances of the word “risk”
- 0 instances of the words “risk treatment”
- 0 instances of the words “risk mitigation”
- 0 instances of the words “risk acceptance”
- 0 instances of the words “risk avoidance”

Evolution of “internal control”

IA focus today is providing subjective opinions on control “effectiveness”

In your organization currently, what areas are Internal audit's time and resources primarily applied to? Please tick the three options that most apply.



Source: State of Internal Audit Survey 2012, Thomson Reuters, p.4

Evolution of “internal control”

Some General Observations:

1. The word “control” is often perceived narrowly and negatively by senior management and work units. Many do not see “controls” as a means to reduce uncertainty/increase certainty of achieving all kinds of business objectives, particularly major value creation objectives.
2. Opining on control “effectiveness” cannot be done in any technically valid way in the absence of clarity on an organization’s risk appetite/tolerance. Few organizations have documented and communicated their risk appetite/tolerance to internal audit.

Evolution of “internal control”

Some General Observations:

3. A large percentage of disputes with management involve disagreements on IA opinions that controls are inadequate/deficient. Stated another way, when IA says there is a “control deficiency” IA is saying they believe the current residual risk status is unacceptable. Deciding on risk appetite is not the remit of IA, it is management and the board’s job.
4. IA rarely examines the full range of “risk treatments” in place when forming opinions on control effectiveness. This can result in wrong opinions and IA distorting optimal corporate resource allocations.

Evolution of “internal control”

Some General Observations:

5. IA rarely provides recommendations on how to “optimize” the current risk treatment strategies.
6. Surveys confirm that a large percentage of IA shops have avoided assessing truly key risk areas. This is caused, at least in part, by the prevailing practice of IA forming subjective opinions on control effectiveness. When IA does ventures in to non-traditional areas (e.g. strategic objectives, M&A, product quality, customer service), and opines on effectiveness of control, the frequency of disputes with management increases.

Evolution of “risk treatments”

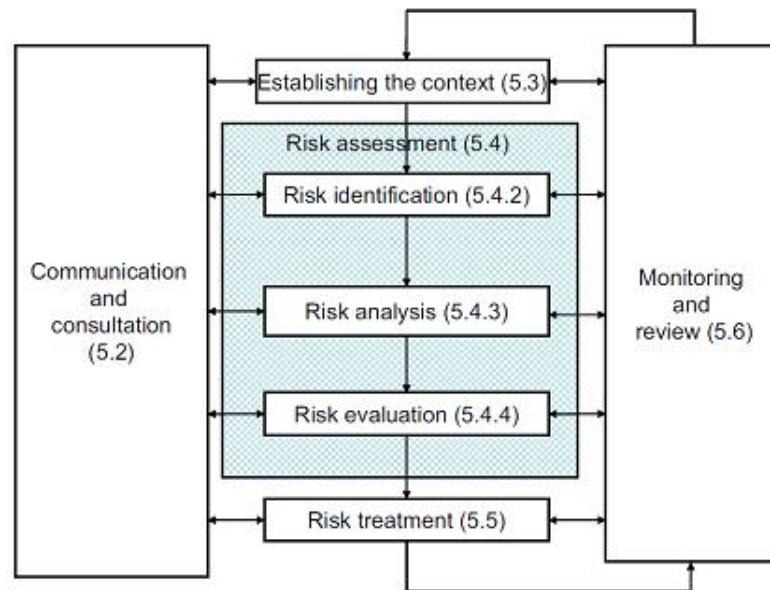


Figure 3 — Risk management process

(Source: International Standard: ISO 31000, Risk management - Principles and Guidelines, 2009-11-15)

Evolution of “risk treatments”

2.25

- **risk treatment**
- process to modify **risk (2.1)**

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 (2.16)**;
- changing the **likelihood (2.19)**;
- changing the **consequences (2.18)**;
- sharing the risk with another party or parties (including contracts and risk financing); and
- retaining the risk by informed decision.

(Source: ISO 31000 2009)

Evolution of “risk treatments”

3.8.1.3 - risk sharing

- form of **risk treatment (3.8.1)** involving the **agreed** distribution of **risk (1.1)** with **other parties**

NOTE 1 Legal or regulatory requirements can limit, prohibit or mandate risk sharing.

NOTE 2 Risk sharing can be carried out through insurance or other forms of contract.

NOTE 3 The extent to which risk is distributed can depend on the reliability and clarity of the sharing arrangements.

NOTE 4 Risk transfer is a form of risk sharing.

(Source: ISO Guide 73 Risk Management Vocabulary, page 10)

Evolution of “risk treatments”

3.8.1.4 - risk financing

form of **risk treatment (3.8.1)** involving contingent arrangements for the provision of funds to meet or modify the financial **consequences (3.6.1.3)** should they occur

(Source: ISO Guide 73 Risk Management Vocabulary, page 11)

Evolution of “risk treatments”

3.8.1.2 - risk avoidance

- informed decision not to be involved in, or to withdraw from, an activity in order not to be exposed to a particular **risk (1.1)**

NOTE Risk avoidance can be based on the result of risk evaluation (3.7.1) and/or legal and regulatory obligations.

(Source: ISO Guide 73 Risk Management Vocabulary, page 11)

Evolution of “risk treatments”

3.8.1.5 - risk retention

acceptance of the potential benefit of gain, or burden of loss, from a particular **risk (1.1)**

NOTE 1 Risk retention includes the acceptance of **residual risks (3.8.1.6)**.

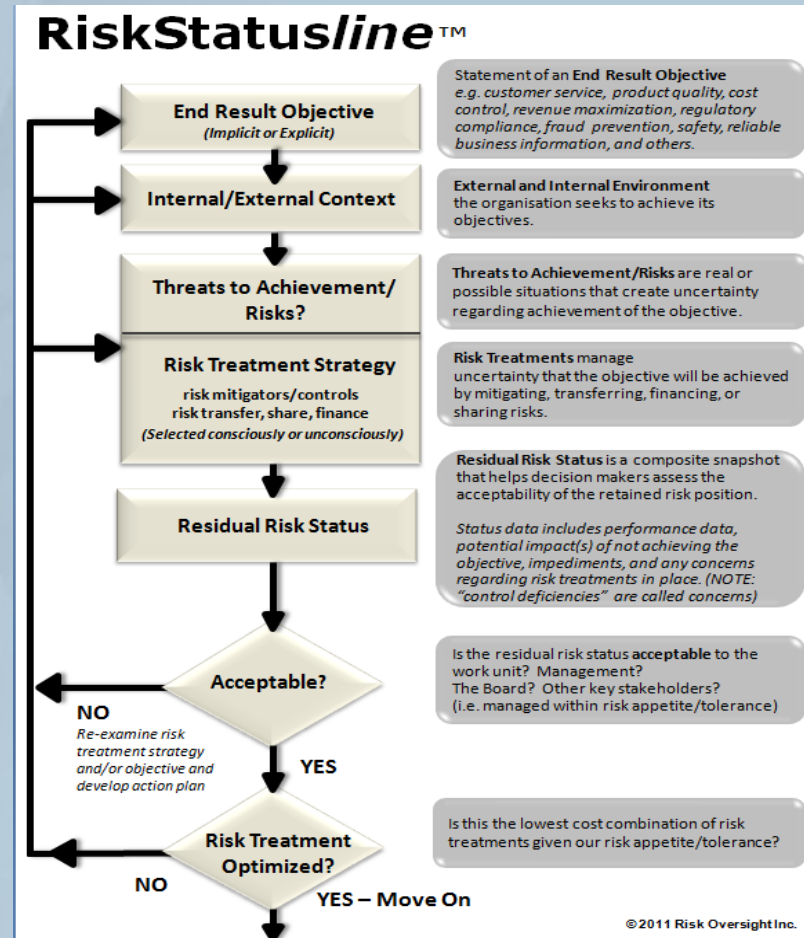
NOTE 2 The **level of risk (3.6.1.8)** retained can **depend on risk criteria (3.3.1.3)**.

(Source: ISO Guide 73 Risk Management Vocabulary, page 11)

Optimizing Risk Treatments

Key goals:

- Consensus agreement on acceptability of residual risk status
- Optimizing risk treatment strategy



Business case for radical change

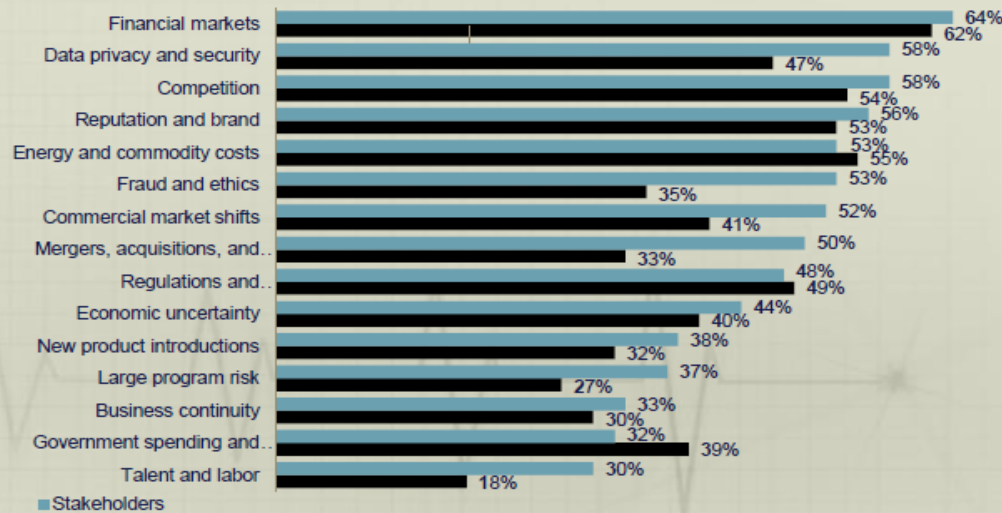
Stated simply, traditional “control centric” “direct report” IA approaches have not worked very well. Key stakeholders are dissatisfied, or worse, dismiss IA as irrelevant. (e.g. new 2012 CICA director guidance)

Significant changes are required to elevate IA’s stature and increase the value added from IA spending.

Transformational change, not incremental change, is required. Slides excerpted from a July 17, 2012 presentation by Richard Chambers, IIA CEO, that follow represent a polite call to action.

Business case for radical change

Risks Are Generally Not Perceived As Well Managed



Source: "Aligning Internal Audit – Are You on the Right Floor? PwC's 2012 State of the Internal Audit Profession Study" © 2012 PricewaterhouseCoopers LLP. All rights reserved. Used with permission.

www.theiia.org/CAE



AUDIT EXECUTIVE
CENTER[®]

(Source: How Resources, Priorities, Opportunities and Challenges Are Aligning for Internal Audit Webinar, Richard Chambers IIA CEO, July 17, 2012)

Business case for radical change

Coverage Still Lags for Two Key Risk Areas



- 58% - No coverage planned in 2012
- 87% - Coverage comprises less than 10% of total audit plan
- 05% - Average allocation of audit plan
- The only good news: 33% are increasing coverage from 2011 levels

Overall Effectiveness of Risk Management

- 57% - No coverage planned in 2012
- 93% - Coverage comprises less than 10% of total audit plan
- 04% - Average allocation of audit plan
- The only good news: 33% are increasing coverage from 2011 levels

120520-EXEC-Pu

www.theiia.org/CAE

(Source: How Resources, Priorities, Opportunities and Challenges Are Aligning for Internal Audit Webinar, Richard Chambers IIA CEO, July 17, 2012)

Business case for radical change

Stakeholder Perceptions: Red Flags for Internal Audit



- Only 59% of stakeholders rate their internal audit function as “somewhat effective” or “very effective” *
- Only 38% of executive stakeholders surveyed believe internal audit frequently delivers insight**
- Almost half of stakeholders responding believe that internal auditing does not excel at developing talent for leadership positions***

Sources:

* Soon to be published results of Ernst & Young's Global Audit Survey

** "Insight: Delivering Value to Stakeholders," © 2011, IIA Research Foundation

*** "A Call to Action: Stakeholders' Perspectives on Internal Auditing," CBOK 2010 © 2011, IIA Research Foundation

120520-EXEC-Pulse-Powerpoint-Slide2.png

www.theiia.org/CAE

.50 in



(Source: How Resources, Priorities, Opportunities and Challenges Are Aligning for Internal Audit Webinar, Richard Chambers IIA CEO, July 17, 2012)

Business case for radical change

Traditional direct report internal audit (i.e. where IA provides subjective opinions on control effectiveness) does not do a good job meeting board risk oversight expectations.

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

- the risk appetite implicit in the company's business model, strategy, and execution is appropriate.*
- the expected risks are commensurate with the expected rewards.*
- management has implemented a system to manage, monitor, and mitigate risk, and that system is appropriate given the company's business model and strategy.*

Business case for radical change

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

- the risk management system informs the board of the major risks facing the company.*
- an appropriate culture of risk-awareness exists throughout the organization.*
- there is recognition that management of risk is essential to the successful execution of the company's strategy.*

Source: National Association of Corporate Directors, REPORT OF THE NACD BLUE RIBBON COMMISSION, RISK GOVERNANCE: BALANCING RISK AND REWARD, October 2009)

Business case for radical change

Key change drivers:

1. Boards of directors, as a result of the 2008 global crisis, now have much greater responsibility for risk oversight and need new and very different information from IA.
2. Organizations need to demonstrate to credit rating agencies, institutional investors, regulators and others that they are effectively managing a wide range of risks.



Business case for radical change

Key change drivers:

3. IIA IPPF standard 2120 **requires** internal audit assess the effectiveness of risk management processes and improve the effectiveness of risk management processes – more subjective IA opinions on control effectiveness and audits that do not use generally accepted risk assessment methods and terminology works against this goal.



Business case for radical change

Key change drivers:

4. It is the responsibility of boards and management to decide on the organization's risk appetite and tolerance. Current IA methods, including subjective opinions on whether controls are, or are not, "effective", cross this line and have often been proved wrong. This causes dysfunctional conflicts and reduces the value that IA can provide.

Business case for radical change

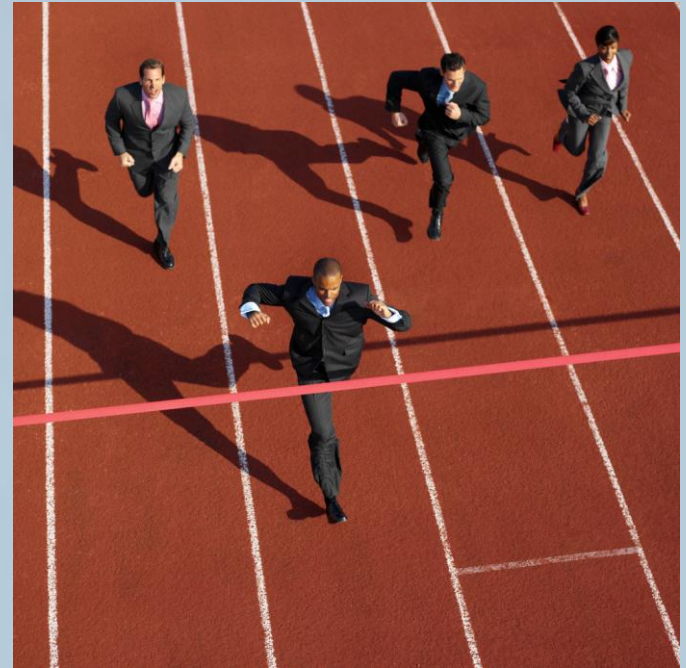
Key change drivers:

5. As a result of the IIA elevating section 2120 of the IPPF standards and launching the CRMA designation in 2011, a growing number of auditors are accepting the premise that IA's primary objective should be "Ensure that senior management and the board are aware of the organization's current residual risk status, including the significant risks being accepted", not spot-in-time, subjective opinions on internal control effectiveness that are often proven wrong on a limited and incomplete universe of business objectives.

Business case for radical change

Key change drivers:

6. Competition – PwC, EY, the IIA and others are conducting surveys and identifying roots of stakeholder dissatisfaction. If IA shops won't change voluntarily other providers will offer services that better meet customer needs and expectations.



The way forward

Transformation Strategy #1

The IIA must continue to elevate the importance of internal auditors helping boards of directors meet new risk oversight responsibilities. Section 2120 is a key element of the way forward.

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

The way forward

Transformation Strategy #2

Adopt ISO 31000
risk assessment
terminology, including
the ISO definition
of “risk”

INTERNATIONAL
STANDARD

ISO
31000

First edition
2009-11-15

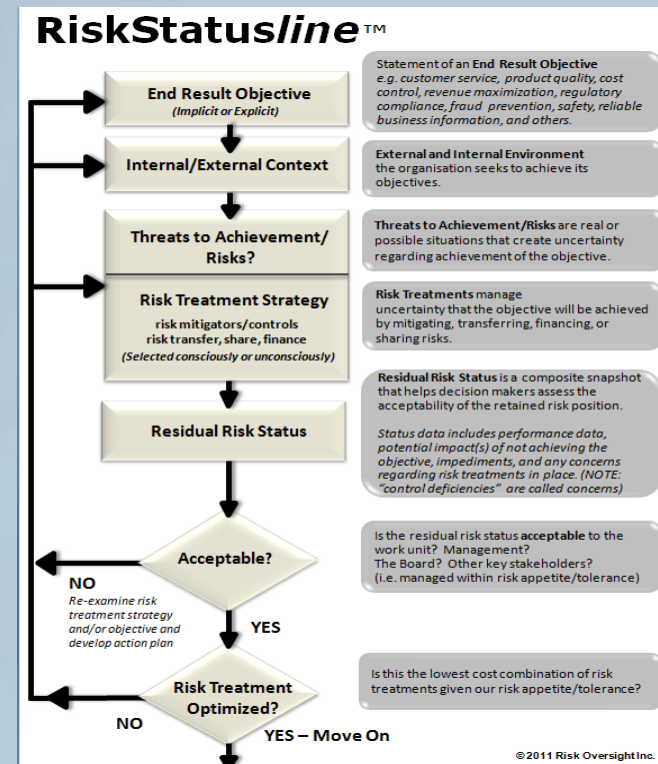
**Risk management — Principles and
guidelines**

Management du risque — Principes et lignes directrices

The way forward

Transformation Strategy #3

Use an objective-centric risk assessment methodology for audits and ERM focused on acceptability of residual risk status



The way forward

Transformation Strategy #4: Move From Supply Driven” To “Demand Driven” Assurance

- Create an “End Result Objectives Register” that includes all important end result objectives necessary for long term success. This “assurance universe” is shared by management and IA
- Assign “Owner/Sponsors” to report upwards on residual risk status using an agreed rating system
- Owner/Sponsors determine the appropriate level of risk. assessment rigor, subject to review by a “Risk Oversight Committee” and the organizations board of directors.
- IA completes risk-based QA reviews on risk status ratings assigned by Owner/Sponsors and assessment work completed.


The way forward

Transformation Strategy #5

Assess how well your organization and IA is doing providing your board of directors with the information they need to meet risk governance expectations

NACD Bookstore

Risk Governance: Balancing Risk and Reward



★★★★★ 5 (1 review)

Series: Blue Ribbon Commission Reports
ISBN: 978-0-943176-45-1
Product Code: BRC-021
Publication Date: 2009

Member Price: \$50.00

[ADD TO CART](#)

The *Report on the NACD Blue Ribbon Commission on Risk Governance: Balancing Risk and Reward* provides a blueprint—practical advice and suggestions—for boards to improve their processes for overseeing the company's risk management activities.

This report includes the following Commission recommendations:

- Before considering how a board should oversee the company's activities to manage risk, it is helpful to consider the goals and objectives of the risk oversight effort. The report outlines important risk oversight objectives which every board should consider in determining how to conduct its oversight activities.
- Without risk, there is no reward, an obvious axiom, but especially valuable today. Understanding the critical link between strategy and risk is essential to effective oversight. An important role for the board is to understand and agree on the company's risk appetite—or the level of risk—that their organization is willing to accept in order to meet its strategic objectives.
- The full board, as well as each of its standing committees, has responsibility for risk oversight. The report weighs the pros and cons of focused committee responsibility versus full board responsibility, and recommends that, as a general rule, the full board should have primary responsibility for risk oversight, including oversight of strategic risk, and the board should assign to its various standing committees responsibility to oversee the risks inherent in their areas of oversight.

QUESTIONS????

tim.leech@riskoversight.ca

www.riskoversight.ca

Twitter: www.twitter.com/riskoversight