risk oversight
A better response to risk.

Board Driven/Objective Centric Internal Audit & ERM: Next Generation Assurance

ACCA Virtual Conference Fall 2013

Presented by Tim Leech FCPA CIA CRMA CCSA CFE Risk Oversight Inc.
www.riskoversight.ca, www.twitter.com/riskoversight

Your Presenter

Tim Leech

Managing Director Global Services

Risk Oversight Inc.

www.riskoversight.ca

tim.leech@riskoversight.ca

risk oversight
A better response to risk.

Agenda

- Evolution of risk oversight expectations
- ERM scorecard to date
- Traditional “Supply Driven” IA/ERM - What’s wrong with the status quo?
- Why Change your IA/ERM approach?
- Board Driven/Objective-centric (“BD/OC”) IA/ERM
- BD/OC IA/ERM – Step by Step
- Business case for BD/OC/ERM & IA
- BD/OC - Next Generation Risk & Assurance Technology
- Questions

Evolution of Risk Oversight Expectations

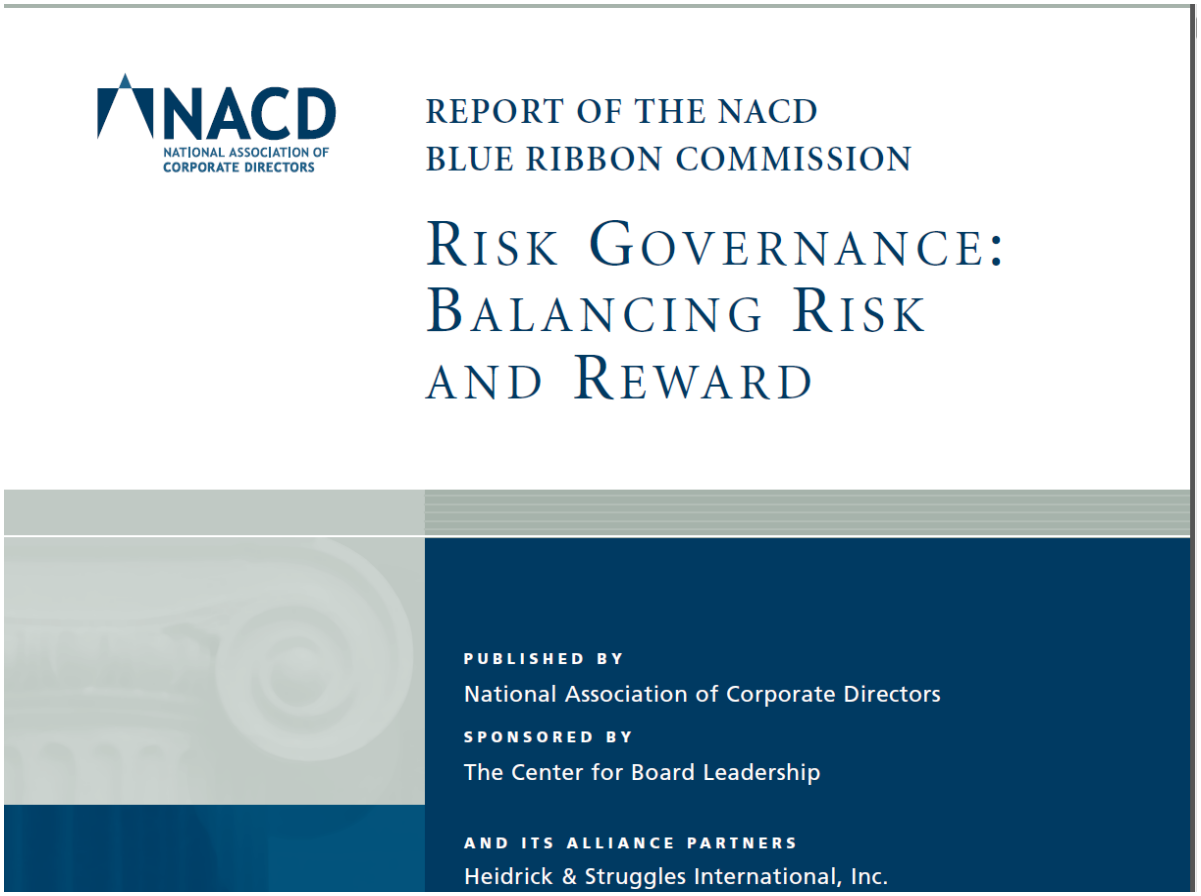
Evolution of Risk Oversight Expectations

Senior Supervisors Group issued three important reports :

1. March 6, 2008 “Observations on Risk Management Practices during the Recent Market Turbulence”
2. October 21, 2009 “Risk Management Lessons from the Global Banking Crisis of 2008”
3. December 23, 2010 “Observations on Developments in Risk Appetite Frameworks and IT Infrastructure”

http://www.newyorkfed.org/newsevents/news/banking/2008/SSG_Risk_Mgt_doc_final.pdf
http://www.newyorkfed.org/newsevents/news_archive/banking/2009/SSG_report.pdf
http://www.newyorkfed.org/newsevents/news/banking/2010/an101223.pdf

Evolution of Risk Oversight Expectations



Evolution of Risk Oversight Expectations

NACD Board Risk Oversight Criteria

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.*

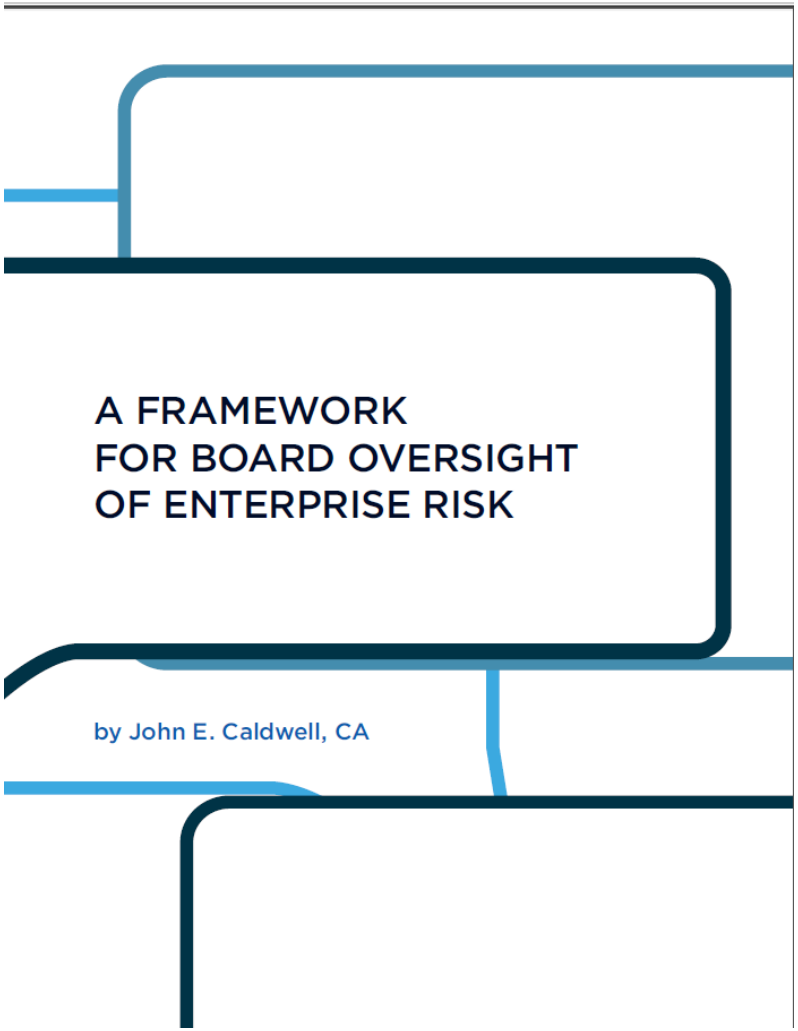
Evolution of Risk Oversight Expectations

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

Evolution of Risk Oversight Expectations



INSTITUTE OF CORPORATE DIRECTORS
INSTITUT DES ADMINISTRATEURS DE SOCIÉTÉS

CA Chartered Accountants of Canada

Evolution of Risk Oversight Expectations

- IIA's IPPF Risk Management Standard 2120 effective 2010 states internal auditors "must" evaluate the effectiveness and contribute to the improvement of risk management processes.

http://www.theiia.org/guidance/standards-and-guidance/ippf/standards/standards-items/?i=8269

Evolution of Risk Oversight Expectations

Per IIA IPPF 2120:

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 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.

http://www.theiia.org/guidance/standards-and-guidance/ippf/standards/standards-items/?i=8269

Evolution of Risk Oversight Expectations

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 December 2, 2010, page24 http://bit.ly/ezvf3O

Evolution of Risk Oversight Expectations

In the U.S. it isn't very clear yet what the SEC wants. It's subject to "best guess" interpretation. Some "best guesses" from informed sources:

Deloitte did research in 2010 and 2011 and has published some criteria for risk oversight disclosures – Risk Intelligent Proxy Disclosures. (http://bit.ly/quRuZN)

PwC has published a summary of opportunities to enhance risk-oversight practices in "Point of View" May 2010. Key conclusions – there should be no ambiguity about the board's responsibility and "the most informative disclosures shed light on relationships and processes". (http://pwc.to/iNBhuJ)

Evolution of Risk Oversight Expectations

FROM THE SEC February 20, 2013:

Item 407(h) also requires companies to describe the role of the board of directors in the oversight of risk. Recently, the U.S. Government Accountability Office found that economic output losses from the 2007-2009 financial crisis could exceed $13 trillion.[16] Given the magnitude of that crisis, which continues to be felt, it would be difficult to overemphasize the importance that investors place on questions of risk management. Has the board set limits on the amounts and types of risk that the company may incur? How often does the board review the company's risk management policies? Do risk managers have direct access to the board? What specific skills or experience in managing risk do board members have? Issuers that offer boilerplate in lieu of a thoughtful analysis of questions such as these have not fully complied with our proxy rules and are missing an important opportunity to engage

Source: SEC Commissioner Speech Louis Aguilar, February 20, 2013
http://www.sec.gov/news/speech/2013/spch022013laa.htm

Evolution of Risk Oversight Expectations

Enterprise Risk Oversight for Directors (EROD):

Enterprise Risk Oversight for Directors course will help directors to better understand how boards and management can more effectively work together to identify, rank and mitigate enterprise risks. This course is based on the CICA publication "A Framework for Board Oversight of Enterprise Risk."

City	Course Date	Application Deadline
Toronto	April 22, 2013	March 28, 2013
Halifax	May 27, 2013	May 2, 2013
Ottawa	May 28, 2013	May 9, 2013
St. John's	May 30, 2013	May 9, 2013
Saskatoon	June 3, 2013	May 9, 2013
Vancouver	June 6, 2013	May 9, 2013
Calgary	June 17, 2013	May 16, 2013

Click here to apply

INSTITUTE OF CORPORATE DIRECTORS
INSTITUT DES ADMINISTRATEURS DE SOCIÉTÉS

Evolution of Risk Oversight Expectations

FRC U.K. Governance Code September 2012

The board is responsible for determining the nature and extent of the significant risks it is willing to take in achieving its strategic objectives. The board should maintain sound risk management and internal control systems. (page 7)

The board should, at least annually, conduct a review of the company's risk management and internal control systems and should report to shareholders that they have done so. The review should cover all material controls, including financial, operational, and compliance controls. (page 18)

Evolution of Risk Oversight Expectations

FRC U.K. Governance Code September 2012

The main role and responsibilities of the audit committee should be set out in written terms of reference and should include:….to review the company's internal financial controls and , unless expressly addressed by a separate board risk committee composed of independent directors, or by the board itself, to review the company's internal control and risk management systems…. To monitor and review the effectiveness of the company's internal audit function. (page19)

Evolution of Risk Oversight Expectations

SAMPLE DISCLOSURE FOR A "RISK COMMITTEE" OF THE BOARD

5. Duties

5.1 Overall

The Committee has oversight of the Risk Management Framework of the Group and specifically the effectiveness of risk management, governance and compliance activity within the Group. The Risk Committee will support the Board in its consideration of the business activities that expose the business to material risks with explicit and dedicated focus on current and forward-looking aspects of risk exposure. It advises the Board on considerations and process for setting the Risk Appetite and related tolerances, taking into account the Board's overall degree of risk aversion and the Company's current financial situation. The Board retains responsibility for approval of the Risk Appetite.

Source: LPEQ Site - Aberdeen Asset Management Plc

http://www.aberdeen-asset.com/aam.nsf/InvestorRelations/termsofreferenceriskcommittee

Evolution of Risk Oversight Expectations

SAMPLE DISCLOSURE FOR A "RISK COMMITTEE" OF THE BOARD

5.2 Risk Appetite

The Group Management Board will define and set the proposed Risk Appetite for the business, with input from the Group Head of Risk. The Risk Appetite being the levels of risk acceptable to the Group in delivering its strategy and is ultimately approved by the Board. The Risk Committee shall on behalf of the Board, review and, if appropriate, challenge the process undertaken by the business in setting this Risk Appetite. The Risk Committee will provide oversight of the process to set and subsequent adhere to the approved risk appetite on a regular basis and at least annually and will make recommendations to the Board.

Source: LPEQ Site - Aberdeen Asset Management Plc

http://www.aberdeen-asset.com/aam.nsf/InvestorRelations/termsofreferenceriskcommittee

ERM Scorecard to Date

ERM Scorecard to Date

The truth is that a large % of ERM initiatives have failed badly or sub-optimized.

<u>Few meet board risk oversight criteria</u> established by the NACD Blue Ribbon Commission "Risk Governance: Balancing Risk and Reward"

ERM Scorecard to Date

2008 Global Financial Crisis –

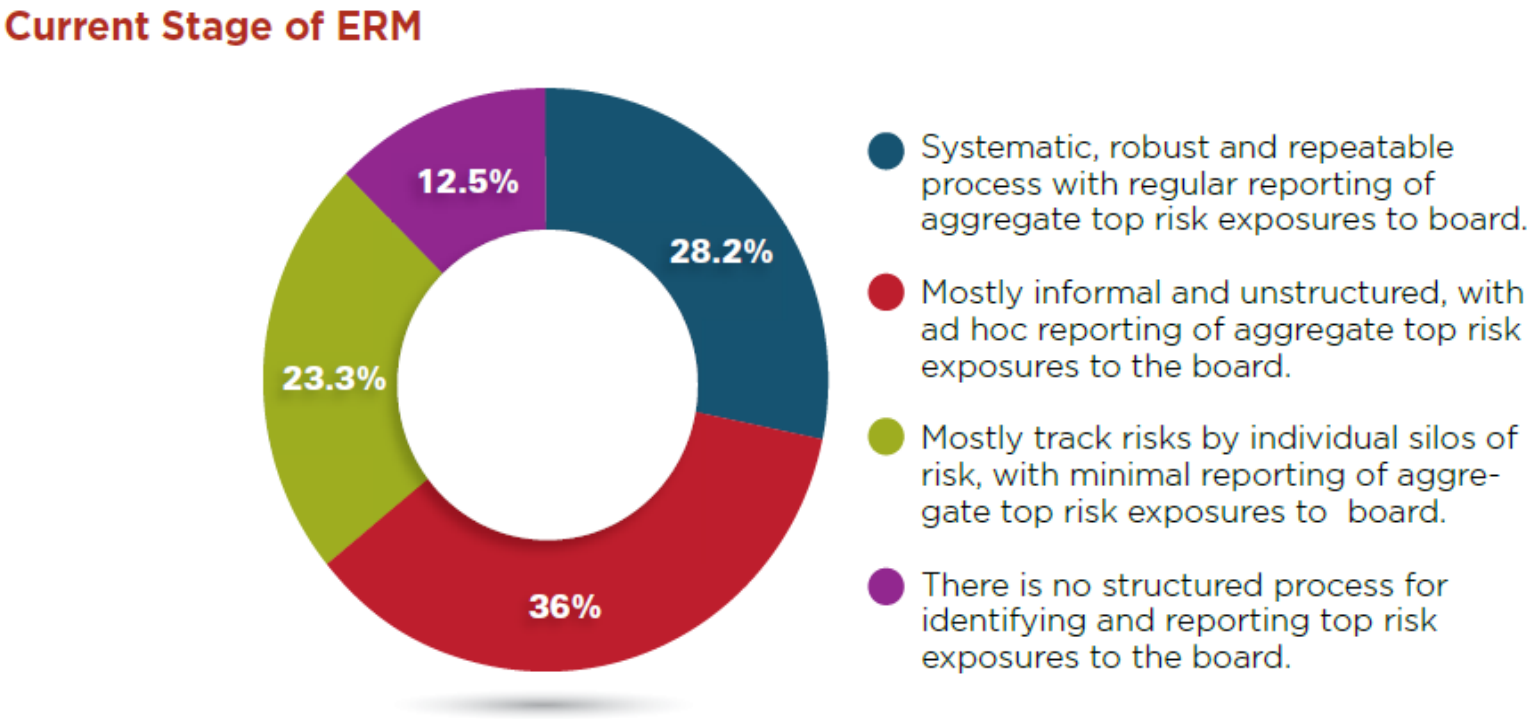
Weak risk management and oversight identified as a root cause of the crisis. But most organizations at the center of the crisis had some form of ERM, and virtually all had large internal audit and IT security functions. Senior Supervisors Group study identified the following root causes in failed institutions:

- *the failure of some boards of directors and senior managers to establish, measure, and adhere to a level of risk acceptable to the firm;*
- *compensation programs that conflicted with the control objectives of the firm;*
- *inadequate and often fragmented technological infrastructures that hindered effective risk identification and measurement; and*
- *institutional arrangements that conferred status and influence on risk takers at the expense of independent risk managers and control personnel.*

Source: Risk Management Lessons from the Global Banking Crisis of 2008, October 21, 2009, Senior Supervisors Group, (http://www.sec.gov/news/press/2009/report102109.pdf)

ERM Scorecard to Date

Limited True Adoption of ERM

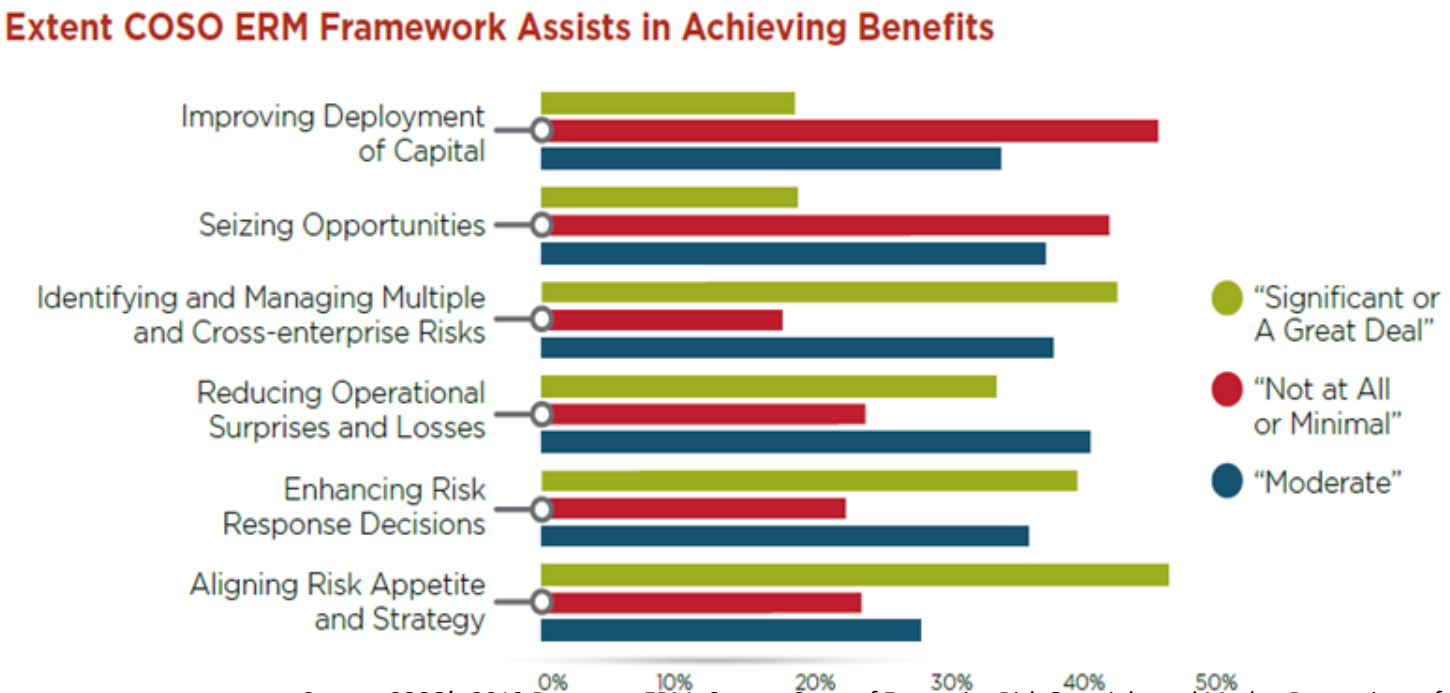


Source: COSO's 2010 Report on ERM: Current State of Enterprise Risk Oversight and Market Perceptions of COSO's ERM Framework

risk oversight
A better response to risk.

ERM Scorecard to Date

COSO 2010 study disclosed that a large % of ERM initiatives were not delivering to a "significant or a great deal" key benefits promised by ERM promoters



Source: COSO's 2010 Report on ERM: Current State of Enterprise Risk Oversight and Market Perceptions of COSO's ERM Framework

risk oversight
A better response to risk.

ERM Scorecard to Date

In Summary:

ERM implementations to date have not delivered promised benefits in a large percentage of organizations around the world; and failed in a spectacular way in dozens of the world's largest and previously respected organizations

UBS

ro risk oversight
A better response to risk.

Traditional “Supply Driven” Assurance: What’s Wrong with the Status Quo?

Traditional "Supply Driven" Assurance: What's Wrong with the Status Quo?

Approach #1: Fund an Internal Audit function/complete audits on a small % of the risk universe/provide opinions on whether control is "effective"

A scene that repeats hundreds of thousands of times around the world:

The chairman of the audit committee extends the thanks of the board for the work done by the Internal Audit department in the previous year and asks two final questions that legal counsel has suggested he pose. He/she inquires:

"Are there any other concerns or control issues that I should be aware of?" "Are controls adequate?"

The chief internal auditor responds:

"I have reported on the issues of significance noted in the year that I think you should be aware of. Management has, for the most part, been very cooperative and has indicated that they will take the steps they consider necessary to rectify the deficiencies noted during our audits. Although we have noted some problems in the course of our audits, overall, controls appear to be adequate in the areas we have reviewed."

Traditional "Supply Driven" Assurance: What's Wrong with the Status Quo?

Approach #2: Internal and external auditors form/report subjective opinions on whether they think controls are "effective" or "adequate"

Question: If the objective is "Prevent/minimize injuries/deaths in the home due to fire", how many "controls" must be present to conclude controls are "effective" or "adequate"?

Should there be a tested escape plan? Should there be a fire extinguisher in the kitchen? In other rooms? Should there be two kinds of smoke detectors, battery and wired? Should there be a fire blanket in the kitchen? Should the house have a sprinkler system? Should parents have burn prevention/treatment training? Should there be an annual inspection by the local fire department or a fire risk specialist? Should there be an annual documented risk assessment that covers statistically probable risks? What about insurance coverage, contractual indemnities with suppliers, etc?

Answer: There is no such thing in real life as "effective controls", only different levels of acceptable retained/residual risk. Auditors and regulators continue to pretend this isn't a fundamental truth.

Traditional "Supply Driven" Assurance: What's Wrong with the Status Quo?

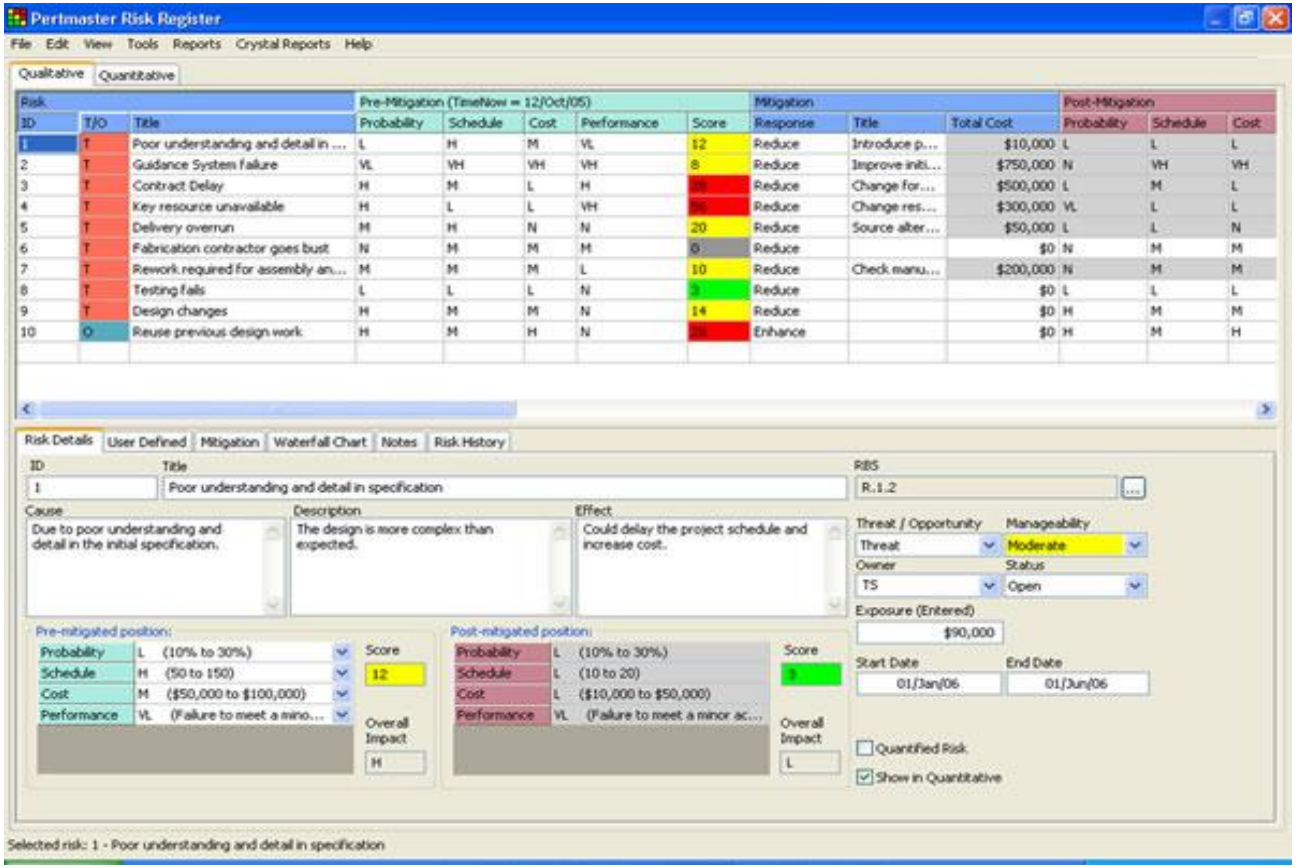
Approach #3: Senior management and boards don't tell Internal Audit with any clarity what they want assurance on and how much

Question: How much should an organization spend on Internal Audit?

Answer: Without reasonable clarity on what senior management and the board want from internal audit, it is possible to propose and defend cost estimates ranging from $50,000 (tokenism) to a very high amount. All would allow the organization to report there is an Internal audit function that does audits, reports audit "findings", and complies with the IIA IPPF standards.

Traditional "Supply Driven" Assurance: What's Wrong with the Status Quo?

Approach #4: Staff groups create/maintain a "Risk Register" /Assign "Risk Owners"/Create "risk heat maps"/Report top risks



risk oversight
A better response to risk.

Traditional "Supply Driven" Assurance: What's Wrong with the Status Quo?

Approach #5: Hire a Chief Compliance Officer and a CRO but don't communicate with clarity the company's appetite/tolerance for violations, fines, jail sentences, or scope of work

Questions: Did the boards of Barclays/RBS/UBS know the bank was engaged in LIBOR manipulation? Should they have known?

Is the LIBOR scandal a failing of Internal Audit? Risk Management? Compliance? Bank boards? or just a bad risk call by management that went badly wrong?

Barclays forced to name executives on Libor list

Recommend 19 people recommend this.

By Matt Scuffham

LONDON | Thu Jan 24, 2013 1:33pm EST

(Reuters) - Barclays was forced to name former heads Bob Diamond and John Varley, finance director Chris Lucas and other top executives and traders linked to a global rate-fixing probe, despite

risk oversight
A better response to risk.

Traditional "Supply Driven" Assurance: What's Wrong with the Status Quo?

Approach #6: Annual reports now include a long list of "risks", including a wide range of IT risks. Regulators are increasingly concerned that these disclosures don't always represent the most important risks that boards should be focusing their attention on and investors should know about

Following the 2008 global financial crisis regulators concluded public companies should report what they see as the biggest risks that could impact the company and describe how the board oversees risk. Most companies now do this in some form. Unfortunately it isn't clear at this point, even to risk experts, if regulators want the biggest inherent/gross risks before considering "risk treatments", or what the company considers the biggest retained/residual risk areas. The FRC in the UK has taken the lead in this area and indicated that a key test from their perspective is whether the board has specifically discussed and agreed the risks that will be disclosed in the annual accounts as the "principle risks and uncertainties" facing the company.

http://www.frc.org.uk/News-and-Events/FRC-Press/Press/2011/February/The-Financial-Reporting-Review-Panel-highlights-ch.aspx

Traditional "Supply Driven" Assurance: What's Wrong with the Status Quo?

Approach #7: Boards place heavy reliance on the company's external auditors when their engagement letters severely limit scope and audit quality is variable

In our opinion, the accompanying consolidated balance sheets and the related consolidated statements of operations, cash flows, changes in equity, and comprehensive income present fairly, in all material respects, the financial position of ***MF Global Holdings Ltd****. and its subsidiaries (the "Company") at March 31, 2011 and 2010, and the results of their operations and their cash flows for each of the three years in the period ended March 31, 2011 in conformity with accounting principles generally accepted in the United States of America. Also in our opinion,* ***the Company maintained, in all material respects, effective internal control over financial reporting as of March 31, 2011****, based on criteria established in Internal Control— Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).*

PRICEWATERHOUSECOOPERS LLP

New York, New York May 19, 2011

PROBLEM: Over 1.6 billion dollars of investor funds couldn't be located shortly after this certification by PwC. This is not an isolated event nor is it meant to single out PwC. The current external audit paradigm has a fairly high error rate that isn't likely to get better anytime soon in the absence of major changes in the auditing standards and methods used. Directors are increasingly expected to demonstrate that they have evaluated the effectiveness of the firm's internal and external auditor s – not a small task in a changing and increasingly complex world.

Traditional "Supply Driven" Assurance: What's Wrong with the Status Quo?

Approach #8: Boards rely heavily on management, often using largely informal approaches without any form of independent assurance, to identify and report areas of high retained risk to the board – how well this happens varies widely

BBC Sign in | News | Sport | Weather | iPlayer | TV | Rad

NEWS BUSINESS

Home | World | UK | England | N. Ireland | Scotland | Wales | Business | Politics | Health | Education | Sci/Envir

Market Data | Your Money | Economy | Companies

6 February 2013 Last updated at 15:12

Share

Libor scandal: RBS fined £390m

Royal Bank of Scotland (RBS) has been fined £390m ($610m) by UK and US authorities for its part in the Libor rate-fixing scandal.

The UK's Financial Services Authority issued a fine of £87.5m, while about £300m will be paid to US regulators and the US Department of Justice.

The fines are £100m greater than those issued to banking rival Barclays last year for similar offences.

RBS chairman Sir Philip Hampton said it was a "sad day" for the bank.

RBS is the third major bank to admit attempting to manipulate the Libor rate

Related Stories

risk oversight
A better response to risk.

Why change your IA/ERM approach?

- Intensifying regulatory pressure on boards post 2008 global crisis to visibly and actively oversee management's risk appetite and tolerance
- Traditional IA/ERM methods weren't designed for, and don't focus on, identifying and communicating the state of residual/retained risk to boards
- Significantly heightened board risk and audit oversight disclosure requirements that are likely to attract even more attention going forward
- Competitive differentiator/escalating client and investor expectations – especially from institutional investors and in high dependency customers/vendor situations
- Cost of capital - credit rating agencies now explicitly consider risk governance (e.g. see S&P expectations http://bit.ly/jScZ9q)

Why change your IA/ERM approach?

- Institutional investors are putting more focus and importance on risk oversight (e.g. ICGN expectations at http://bit.ly/e7tSFu)

- Increased senior management and board confidence key value creation objectives will be achieved and major value eroding events avoided or mitigate

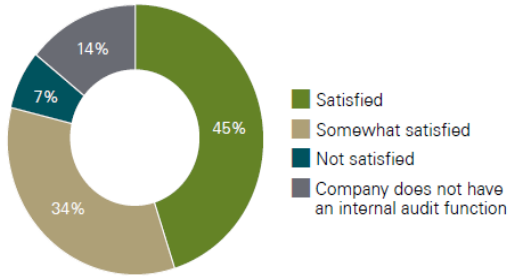
- Current risk management/assurance approaches continue to allow major negative events/value erosion and all too often don't work very well

- Strong regulatory push globally for public disclosure of "Risk appetite/risk framework statements" especially for financial insitutions (e.g. see OSFI risk appetite statement expectations in Annex B (http://bit.ly/YG1vp1)

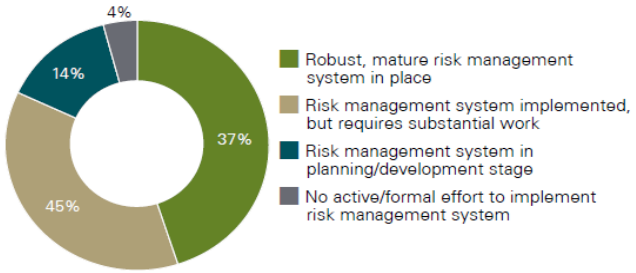
Why change your IA/ERM approach?

A lot of dissatisfied customers

Q14. How satisfied are you that your company's internal audit function delivers the value to the company that it should?



Q18. What is the status of your company's risk management program?



(Source: KPMG Global Audit Committee Survey January 2013 http://bit.ly/WHeaoc)

risk oversight
A better response to risk.

Board Driven/Objective Centric Internal Audit /& ERM

Board Driven/Objective Centric IA & ERM

- Clearly defined risk management and risk oversight accountabilities up to and including the Board. The Board demands reliable information on significant **retained/residual risk status linked to important value creation and potential value erosion objectives** from management, and assurance on reliability from IA and ERM staff groups.

- Board plays an active and visible role overseeing effectiveness of enterprise-wide risk management processes and management's risk appetite/tolerance

- CEO or his/her designate (the CRO when one exists) is responsible for providing the board with a consolidated report on the state of residual risk. This includes objectives that currently have significant unacceptable residual risk status, as well as objectives that have a high level of retained/residual risk but have been rated by management as acceptable/within the company's risk appetite/tolerance

Board Driven/Objective Centric IA & ERM

- The "Risk Oversight Committee" selected by the CEO oversees implementation and maintenance of the company's risk management framework, quality of the reports on residual risk status to the board, deciding which objectives warrant formal assurance, assigning objectives to "OWNER/SPONSORS", and agreeing risk acceptance decisions made by OWNER/SPONSORS.

- OWNER/SPONSORS must report on the state of residual risk status on the objectives they are assigned and the appropriate level of risk assessment rigor. If they believe they need help to meet their responsibilities it is up to them to request training and/or facilitation services and/or have a third party complete the risk assessment for them.

- "Risk & Assurance Unit"/ "ERM Support Services" (which may be part of IA subject to caveats) has responsibility for creating and maintaining the risk assessment/risk status reporting processes

Board Driven/Objective Centric IA & ERM

- Internal Audit or equivalent reports on reliability of risk management processes and the risk assessments completed, as well as objectives that it believes should be included in the OBJECTIVES REGISTER but were not, and where it believes higher/better risk assessment rigour than the risk assessment choice selected by OWNER/SPONSOR is warranted. (e.g. OWNER SPONSOR may have selected 2 minute risk assessment rigor level and IA thinks it warrants 2 day rigor level)

- Internal audit uses the OBJECTIVES REGISTER as the core foundation for its assurance work and annual work plans. It can request specific residual risk status information be elevated to the board for consensus agreement and can report instances where it believes the residual risk status data is unreliable.

- An external specialist may be engaged periodically to report on reliability of the company's risk management/risk oversight framework especially if IA plays a key role launching/maintaining/actually completing risk management processes

Implementing Board Driven/Objective Centric IA & ERM: Step-by-Step

- Drafting/approving Corporate Risk Policy
- Populating your “OBJECTIVES REGISTER”
- Assigning “OWNER/SPONSORS”
- Training OWNER/SPONSORS
- RiskStatusline™ assessment method
- Deciding on risk assessment rigor level
- Assigning “Residual Risk Ratings” (“RRRs”)
- Preparing consolidated entity-level risk reports
- IA assesses reliability of process and output

Implementing Board Driven/Objective Centric IA & ERM: Corporate Risk Policy

Policy Overview

- PURPOSE
- SCOPE
- RISK MANAGEMENT PRINCIPLES
- CORPORATE RISK ASSESSMENT METHODOLOGY
- RISK MANAGEMENT ROLES AND RESPONSIBILITIES
  - Board of Directors/Audit Committee
  - CEO
  - Risk Oversight Committee
  - Heads of Departments
  - Compliance & Risk Department

(For a free sample Demand Driven policy contact tim.leech@riskoversight.ca)

Implementing Board Driven/Objective Centric IA & ERM: Populating Objective Registers

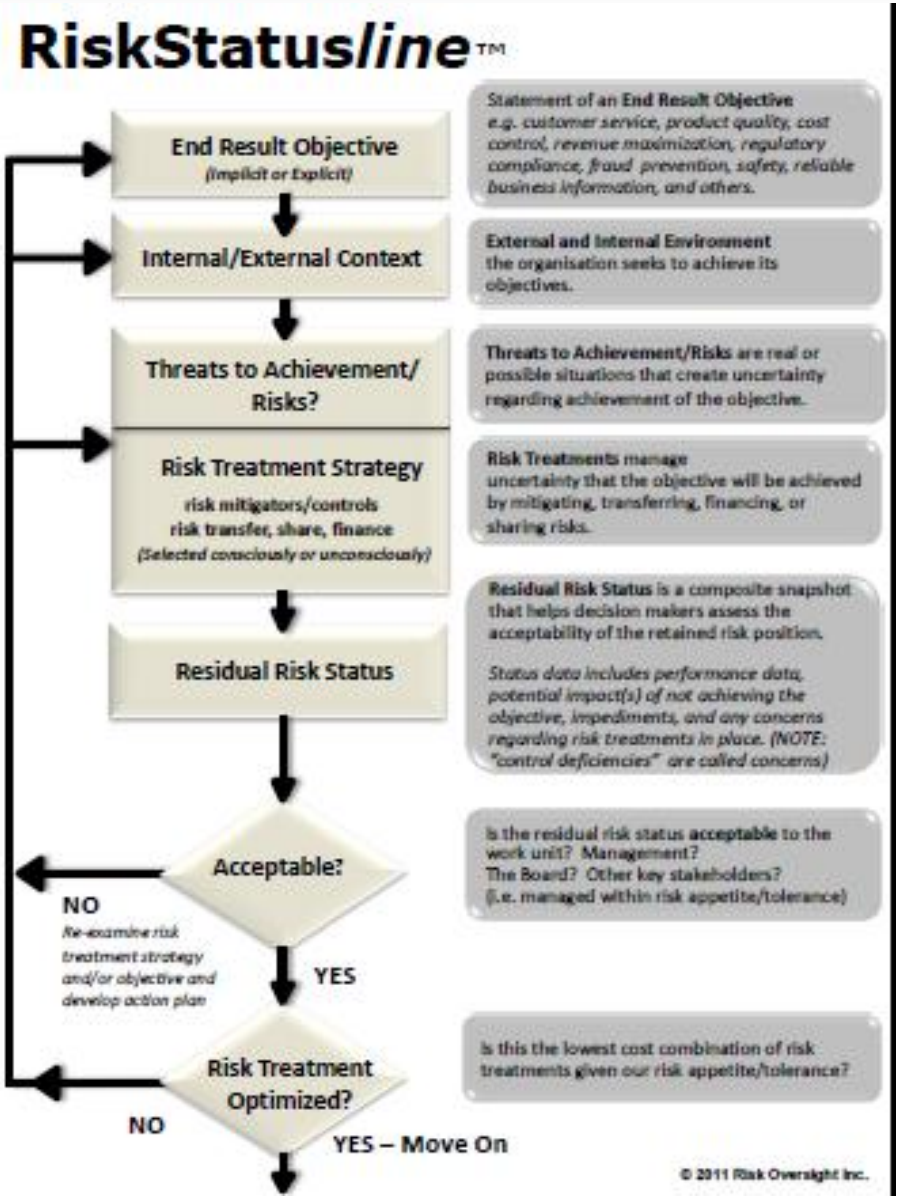
Core Principles

1. Only objectives senior management and/or the board want formal assurance on should be included. Formal assurance costs money and this decision should be made consciously by key customers.
2. At minimum the entity's top value creation objectives and objectives that could result in significant value erosion/reputation damage should be included.
3. Traditional internal audit universes and risk registers can be "reverse engineered" to identify the linked end result objectives. Often these have not included strategic objectives/top value creation objectives

Core Principles

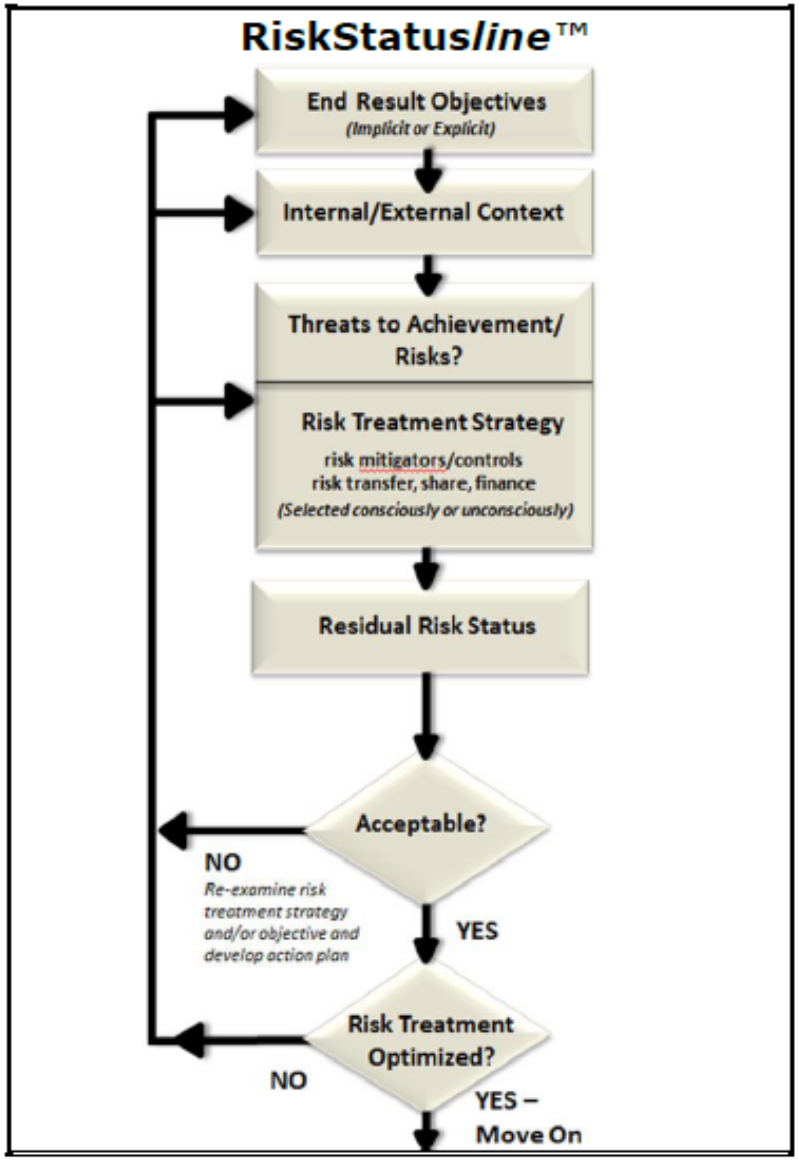
4. The top value creation objectives should be sourced from the organization's strategic plans and budgets, executive compensation metrics (including the CEO's), publicly disclosed objectives/strategies, and other available sources.
5. Top potential value erosion objectives can be identified via research – which events, other than flawed strategy/strategy execution, could lead to significant value erosion? This will category will include objectives linked to major legal violations, fraudulent /unreliable financial statements, environmental incidents, major safety incidents, lawsuits for breach/negligence, cyber security, data loss/corruption, programs that don't do what they should, etc

Implementing Board Driven/Objective Centric IA & ERM: RiskStatus*line*™ Assessment Method



risk oversight
A better response to risk.

Implementing Board Driven/Objective Centric IA & ERM: Assigning Residual Risk Rating



RESIDUAL RISK RATING DEFINITIONS

0 Fully Acceptable – Residual risk status is acceptable. No changes to risk treatment strategy required.

1 Low - Inaction on unacceptable terms could result in very minor negative impacts. Ad hoc attention may be required to adjust status to an acceptable level.

2 Minor – Inaction or unacceptable terms could result in minor negative impacts. Routine management attention may be required to adjust status to an acceptable level.

3 Moderate - Inaction on unacceptable risk status could result in or allow continuation of mid-level negative impacts. Moderate senior management effort required to adjust status to an acceptable level.

4 Advanced – Inaction or unacceptable risk status could allow continuation of /or exposure to serious negative impacts. Senior management attention required to adjust risk status.

5 Significant - Inaction on unacceptable risk status could result in or allow continuation of very serious negative impacts. Attention required to adjust status to an acceptable level.

6 Major - Inaction on unacceptable risk status could result in or allow continuation of very major entity level negative consequences. Analysis and corrective action required immediately.

7 Critical - Inaction on unacceptable risk status virtually certain to result in or allow continuation of very major entity level negative consequences. Analysis and corrective action required immediately.

8 Severe - Inaction on unacceptable risk status virtually certain to result in or allow continuation of very severe negative impacts. Senior board level attention urgently required.

9 Catastrophic - Inaction on unacceptable risk status could result in or allow the continuation of catastrophic proportion impacts. Senior board level attention urgently required to avert a catastrophic negative impact on the organization.

10 Terminal - The current 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 to prevent the demise of the entity.

Implementing Board Driven/Objective Centric IA & ERM: Assigning Residual Risk Rating

When a decision is made to include an objective in the "OBJECTIVE REGISTER" the "OWNER/SPONSOR" must assign a "RESIDUAL RISK RATING" to the objective and decide on the level of risk assessment rigour from very low (takes minutes) to very high rigour. These scores must be revisited periodically and adjusted by the OWNER/SPONSOR as formal risk assessments are done and/or new information emerges

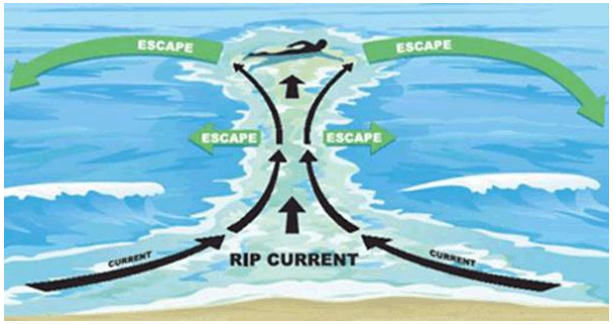
risk oversight
A better response to risk.

Implementing Board Driven/Objective Centric IA & ERM: Deciding on Risk Assessment Rigour

Risk*Status* Analysis Level	Overview of Assessment Options
Quick Start	• Define/refine end result business objectives and "Owner/Sponsors" • Assign an initial Residual Risk Status rating for each objective from 0 (fully acceptable) to 10 (entity catastrophic) The rating is linked to the level of management/board attention.
Importance Prioritization Option	• Quick Start requirements (see above) • Assign an objective importance rating – importance to the unit • Assign an objective importance rating – importance to the entire corporation • Document current level of risk status knowledge and target level. The higher the gap between current and target the higher the objective's priority.
High Level Risk Assessment	• Quick Start and Importance Prioritization options (see above) • Document threats to achievement/risks, likelihood and consequences of risks, and risk level • Document "best guess" current mitigation estimate for each threat/risk and traffic light rating • Develop and assign responsibility for risk treatment action items for risks with unacceptable residual risk ratings
Full RiskStatus*line*™ Assessment	All steps above plus: • Document key risk treatments in place to manage significant risks • Document current performance information for the objective using best available information ("KPI" information) • Document impact information for the objective including what would be the consequences to company, unit, individuals, community etc if the objective wasn't achieved in whole or part. (NOTE: This is impact of non-achievement of objective not individual risks impacts) • Document known concerns – risk treatments/controls known to be missing, deficient or needing improvement • Document any impediments - elements outside of the control/ resources of the business objective owner that would prevent them from adjusting retained risk level • Assign action items

Implementing Board Driven/Objective Centric IA & ERM: Consolidated Report on Risk

Very simply, consolidated residual risk reports provide details on important value creation and potential value erosion objectives that have high residual risk ratings. (see prior slides) High RRRs indicate increasingly material unacceptable retained risk positions with potential to have a significant negative impact on the achievement of specified end result objectives.



Business Case for Board Driven/Objective Centric Internal Audit & ERM

1. Primary responsibility for risk management, risk assessment, and risk reporting is positioned squarely with management.
2. Boards are provided with more reliable, quality assured entity level information on the current state of residual/retained risk. This helps boards understand and oversee management's risk appetite and tolerance.
3. The approach focuses attention on the upside of risk management by emphasizing the need to include the company's top value creation objectives in the OBJECTIVES REGISTER. OWNER/SPONSORS of those objectives are incentivized to use risk assessment tools to increase certainty/reduce uncertainty that top value creation objectives and potentially value eroding objectives will be achieved while still operating within a tolerable level of retained/residual risk.

Business Case for Board Driven/Objective Centric Internal Audit & ERM

4. Allows an organization to make conscious, visible, well thought-out decisions on which business objectives warrant the cost of formal assurance/risk management and how much assurance is required.
5. Uses globally accepted ISO 31000/Guide 73 terminology for risk assessments.
6. Encourages users to consider not only the acceptability of the residual/retained risk status, but also whether the current "risk treatments in place are optimized – i.e. the lowest possible cost combination that would still produce an acceptable level of residual risk.
7. Links performance information on specific objectives to related risks and risk treatments allowing users to see the impact of any changes made to the risk treatment design.

Business Case for Board Driven/Objective Centric Internal Audit & ERM

8. Internal audit departments are provided with clear requirements from senior management and/or the board detailing which objectives they want formal assurance on and how much. This helps estimate what internal audit's annual budget should be. IA's main role is to provide assurance/opinions on the reliability of the entity's risk assessment processes, and the consolidated report on residual risk status for the board of directors.
9. ERM support teams are provided with clear deliverables that detail which objectives senior management and/or the board want risk status information and the level of target level of risk assessment rigor. The onus is on OWNER/SPONSORS to request training/facilitation/assessment assistance from the ERM support team to support risk assessment rigor decisions OWNER/SPONSORS, the Risk Oversight Committee, and/or the board have decided is warranted.

Board Driven/Objective Centric
"Next Generation" Technology

Resolver and Risk Oversight Inc. have partnered to bring "Next Generation" risk and assurance software to market using the board driven/objective centric approach

NAME OF THE SOFTWARE: RiskStatusNet™

UNDERLYING METHODOLOGY: RiskStatusOversight™ - Board Driven/Objective Centric

BETA TESTING LAUNCH DATE: April/May 2013

Thank you/Questions???

Tim Leech

tim.leech@riskoversight.ca

www.riskoversight.ca

Twitter: www.twitter.com/riskoversight

risk oversight
A better response to risk.