Board Oversight of Risk Culture, Appetite & Tolerance: What Companies Need to do to Respond

Tim Leech FCPA CIA CRMA CFE
Risk Oversight Solutions Inc.
www.riskoversightsolutions.com

© Risk Oversight Solutions Inc.
About Your Presenter

Tim J. Leech, FCPA CIA CRMA CCSA CFE is Managing Director at Risk Oversight Solutions Inc. based in Oakville, Ontario 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 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 training 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” and co-author of the highly acclaimed January 2014 “Risk Oversight: Evolving Expectations for Boards”. Leech was a pioneer in the global control and risk self-assessment (“CRSA/CSA”) movement from 1996 to 2004. His latest ground breaking article, “Reinventing Internal Audit”, is scheduled for release April 1, 2015 in the IIA’s Internal Auditor magazine.

In 2013 he launched a second generation of disruptive innovation with a breakthrough approach to risk and assurance management – “Board & C-Suite Driven/Objective-centric” risk governance. 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 is currently working with Resolver in Toronto, Canada to build RiskStatusNet™ software to support full integration of what is sometimes referenced as the five lines of defence. Beta testing is currently underway.

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

- Codification of board risk oversight expectations
- Board oversight of “risk culture” – the new frontier
- Barriers to effective board oversight of risk
- Board & C-Suite driven/Objective centric (“BD/OC”) risk and assurance core concepts
- The way forward
- Questions
Codification of Board Risk Oversight Expectations

March 14, 2008 12:03 P.M. ET

Bear Stearns bailout
J.P. Morgan and N.Y. Fed provide funds to strapped Wall St broker

Extraordinary action taken after Bear Stearns by CEOs' admission
An offer is significant 24-hour intervention in its liquidity position
J.P. Morgan statement suggests an end game is yet to play out

• Bailout offers $2 (First Time)
• Bear Stearns (Strapped Wall Street)
• Parallels in history: (Collapsing)
• Choose the Bear Stearns news
• Breaking-news alerts via email

MARCH SNAPSHOT: STREET REACTS TO BAILOUT | Markets

• Bailout news details U.S. stocks
• Nears & Nears for Friday
• Treasury action reflects concern
• Fed funds futures point to higher likelihood of a 50 point rate cut

• Dollar gains up further ground
• Gold edges to record $695
• Crude oil drops to $51.90 per

ELSEWHERE IN FINANCIALS
• Subprime Today — Not So Slowdown
• Countrywide fights federal probe
• Credible Capital investors may not be stuck
• Security Capital asks auditor warning
• Hedge firm RAL's shares rise on results
• Bank to permaulk of Visa's IPO proceeds

AIG

UNDER NEW MANAGEMENT — YOU
JUST BOUGHT IT!

So long, Bear Stearns

BSC

Final bid, $2

The TIme

Lehman collapse sends
shockwave round world
Codification of Board Risk Oversight Expectations
Codification of Board Risk Oversight Expectations

REPORT OF THE NACD
BLUE RIBBON COMMISSION

RISK GOVERNANCE:
BALANCING RISK
AND REWARD

PUBLISHED BY
National Association of Corporate Directors
SPONSORED BY
The Center for Board Leadership
AND ITS ALLIANCE PARTNERS
Heidrick & Struggles International, Inc.
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.
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.

Codification of Board Risk Oversight Expectations

A FRAMEWORK FOR BOARD OVERSIGHT OF ENTERPRISE RISK

by John E. Caldwell, CA

© Risk Oversight Solutions Inc.
• 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
**Codification of Board 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.

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
In the U.S. it isn’t very clear yet what the SEC wants/requires. It’s subject to “best guess” interpretation. Some “best guesses” from informed sources:


**PwC** has published a useful risk governance disclosure guide focused on risk management and oversight principles being promoted by the Financial Stability Board. ([http://pwc.to/1ixmFvv](http://pwc.to/1ixmFvv))
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. 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
Financial Stability Board ("FSB") November 2013:

4.1 The board of directors should:

a) approve the financial institution’s RAF, developed in collaboration with the CEO, CRO and CFO, and ensure it remains consistent with the institution’s short- and long-term strategy, business and capital plans, risk capacity as well as compensation programs;

b) hold the CEO and other senior management accountable for the integrity of the RAF, including the timely identification, management and escalation of breaches in risk limits and of material risk exposures;

c) ensure that annual business plans are in line with the approved risk appetite and incentives/disincentives are included in the compensation programmes to facilitate adherence to risk appetite;

d) include an assessment of risk appetite in their strategic discussions including decisions regarding mergers, acquisitions, and growth in business lines or products;

e) regularly review and monitor the actual risk profile and risk limits against the agreed levels (e.g. by business line, legal entity, product, risk category), including qualitative measures of conduct risk;

f) discuss and monitor to ensure appropriate action is taken regarding “breaches” in risk limits;

g) question senior management regarding activities outside the board-approved risk appetite statement, if any;

h) obtain an independent assessment (through internal assessors, third parties or both) of the design and effectiveness of the RAF and its alignment with supervisory expectations;
Codification of Board Risk Oversight Expectations

**Financial Stability Board ("FSB") November 2013:**

4.6 Internal audit (or other independent assessor) should¹³:

a) routinely include assessments of the RAF on an institution-wide basis as well as on an individual business line and legal entity basis;

b) identify whether breaches in risk limits are being appropriately identified, escalated and reported, and report on the implementation of the RAF to the board and senior management as appropriate;

c) independently assess periodically the design and effectiveness of the RAF and its alignment with supervisory expectations;

d) assess the effectiveness of the implementation of the RAF, including linkage to organisational culture, as well as strategic and business planning, compensation, and decision-making processes;

e) assess the design and effectiveness of risk measurement techniques and MIS used to monitor the institution’s risk profile in relation to its risk appetite;

f) report any material deficiencies in the RAF and on alignment (or otherwise) of risk appetite and risk profile with risk culture to the board and senior management in a timely manner; and

g) evaluate the need to supplement its own independent assessment with expertise from third parties to provide a comprehensive independent view of the effectiveness of the RAF.
Codification of Board Risk Oversight Expectations

September 2014

Guidance on Risk Management, Internal Control and Related Financial and Business Reporting
Board responsibilities per FRC UK Sept 2014 Code

Boards are responsible for:

• determining the extent to which the company is willing to take on risk (its “risk appetite”);
• ensuring that an appropriate “risk culture” has been instilled throughout the organization;
• identifying and evaluating the principal risks to the company’s business model and the achievement of its strategic objectives, including risks that could threaten its solvency or liquidity;
• agreeing how these risks should be controlled, managed, or mitigated;
Codification of Board Risk Oversight Expectations

Board responsibilities per FRC UK Sept 2014 Code.

Boards are responsible for (continued):

- ensuring an appropriate risk management and internal control system is in place, including a reward system;
- reviewing the risk management and internal control systems and satisfying itself that they are functioning effectively and that corrective action is being taken where necessary; and
- taking responsibility for external communication on risk management and internal control.

Guidance on Supervisory Interaction with Financial Institutions on Risk Culture: A Framework for Assessing Risk Culture

Available as: PDF

7 April 2014

Abstract

Weaknesses in risk culture are often considered a root cause of the global financial crisis, headline risk and compliance events. A financial institution’s risk culture plays an important role in influencing the actions and decisions taken by individuals within the institution and in shaping the institution’s attitude toward its stakeholders, including its supervisors. First and foremost, it should be expected that employees in all parts of the institution conduct business in a legal and ethical manner. An environment that promotes integrity should be created across the institution as a whole, including focusing on fair outcomes for customers.
2) Consider including or referencing additional guidance that would be useful to both the institution and the supervisor, when applying this particular guidance. For example,

Within section three on “General Supervisory Guidance”, the Consultative Document states, “In particular, supervisors should assess how the board and senior management systematically assess the risk culture of the institution, and document what they are finding and how any deficiencies in risk culture are addressed. The institution’s willingness to sufficiently document the elements supporting its risk culture should form part of the supervisor’s overall assessment.” We suggest that additional guidance may be necessary to supplement a supervisor’s ability to successfully assess an institution’s risk culture, document findings, review remediation plans and determine an institution’s willingness to document elements of its own risk culture.

Please do not hesitate to contact Glenn Darinzo, IIA’s Director of Standards and Guidance, if you have any questions about this response and/or would like to schedule a time for us to either meet in person or via conference call. Mr. Darinzo can be reached via email: glenn.darinzo@theiia.org or phone 1-407-937-1164.

Again we applaud the efforts of the FSB to promulgate guidance for the promotion of a sound risk culture within financial institutions. I look forward to an opportunity to meet you in the future to continue our discussions and further build awareness of the critical role internal auditing can and does play in ensuring good governance, risk management and internal controls thereby enhancing financial stability within financial institutions and other organizations.

Best Regards,

Richard F. Chambers, CIA, CGAP, CCSA, CRMA
President and Chief Executive Officer
Board Oversight of “Risk Culture”: the new frontier

CULTURE AND THE ROLE OF INTERNAL AUDIT
LOOKING BELOW THE SURFACE
Barriers to Effective Board Oversight of Risk
Board Risk Oversight Handicap #1

Rethinking the Risk Agenda: Asymmetric Information Risk

One of the most critical roles of the board of directors is to provide strategic oversight to management. However, directors serve in a part-time capacity while the management team is full time. Inherently, senior-level executives have a much deeper knowledge about the organization’s operational processes and risks than the board. As such, directors rely on senior management for information necessary to carry out their oversight responsibilities.

Asymmetric Information Risk

This inherent imbalance in the information relationship between management and the board is what we call asymmetric information risk.
Barriers to Effective Board Oversight of Risk

Board Risk Oversight Handicap #2

Lack of consensus on what it means
Barriers to Effective Board Oversight of Risk

Board Risk Oversight Handicap #3

Traditional ERM not delivering what’s needed
Barriers to Effective Board Oversight of Risk

Board Risk Oversight Handicap #3

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.

Traditional ERM not delivering what’s needed
Board Risk Oversight Handicap #4

Traditional “Supply Driven” Assurance

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 cover 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.
Barriers to Effective Board Oversight of Risk

Board Risk Oversight Handicap #5

Lack of agreement on what is “effective” risk oversight
Barriers to Effective Board Oversight of Risk

Board Risk Oversight Handicap #6

Litigation risk: “Damned if we do/Damned if we don’t”
Barriers to Effective Board Oversight of Risk

Board Risk Oversight Handicap #7

Lack of effective integration – risk silos turf wars
Barriers to Effective Board Oversight of Risk

Board Risk Oversight Handicap #8

Boards have not asked/demanded what they need
Board & C-Suite Driven/Objective Centric Risk Governance
Transform risk and assurance functions from “supply driven” to “board/C-Suite driven”. The end game - seek conscious consensus agreement on acceptability of the company’s retained/residual risk status, the level of risk assessment rigour and level of independent assurance senior management and the board wants and is prepared to pay for.

Clarify accountabilities - Clearly defined risk management and risk oversight accountabilities up to and including the Board. In this model the Board demands reliable information on significant retained/residual risk status linked to important value creation and potential value erosion objectives from the CEO and management. IA and ERM function, if one exists, provide independent reports on management’s report on risk status to the board.

Focus on end-result objectives and creating a clear picture of the current consolidated residual risk status linked to key objectives.
Change internal audit’s mandate and reporting. Internal audit’s primary mandate is to ensure senior management and the board are aware of the current residual risk status linked to key value creation and potential value erosion objectives and help improve the organization’s risk management processes.

Change the mandate of ERM functions. ERM functions should be tasked with creating and maintaining reliable processes capable of providing materially reliable status reports on the current state of retained/residual risk linked to key value creation and potentially value erosion objectives.

Demand better information on risks posed by reward systems. Misaligned reward systems have been at the root of many of the biggest governance failures in history.
• **Recognize the need for training.** Current approaches to ERM, internal audit, compliance, safety, environment don’t provide the information necessary for boards to discharge their responsibility to oversee management’s risk appetite and tolerance. Training and new IT systems are required.

• **Recognize and accept that better documented risk management is a “two-edged sword”**. Most companies in the world today break at least some laws, sometimes a little and sometimes a lot. Some manage earnings. Sometimes a little, and sometimes a lot. Others sacrifice safety and the environment for profits. Sometimes plausible deniability is the best defence boards can present. Delaware Courts in the U.S. and elsewhere are still fairly receptive to the “I didn’t know” defence.
Implementing Board & C-Suite Driven/Objective Centric: Use ‘Objective Centric’ Risk Assessment

RiskStatusline™

- End Result Objective
  - (Implicit or Explicit)
  - Internal/External Context
  - Threats to Achievement/Risks?
  - Risk Treatment Strategy
    - risk mitigators/controls
    - risk transfer, share, finance
      - (Selected consciously or unconsciously)
  - Residual Risk Status

- Acceptable?
  - NO: Re-examine risk treatment strategy and/or objective and develop action plan
  - YES: Risk Treatment Optimized?
    - NO
    - YES – Move On

- Statement of an End Result Objective
  - e.g. customer service, product quality, cost control, revenue maximization, regulatory compliance, fraud prevention, safety, reliable business information, and others.

- External and Internal Environment
  - the organisation seeks to achieve its objectives.

- Threats to Achievement/Risks are real or possible situations that create uncertainty regarding achievement of the objective.

- Risk Treatments manage uncertainty that the objective will be achieved by mitigating, transferring, financing, or sharing risks.

- Residual Risk Status is a composite snapshot that helps decision makers assess the acceptability of the retained risk position.

- Status data includes performance data, potential impact(s) of not achieving the objective, impediments, and any concerns regarding risk treatments in place. (NOTE: “control deficiencies” are called concerns)

- Is the residual risk status acceptable to the work unit? Management? The Board? Other key stakeholders? (i.e. managed within risk appetite/tolerance)

- Is this the lowest cost combination of risk treatments given our risk appetite/tolerance?

© Risk Oversight Solutions Inc.
Implementing Board & C-Suite Driven/Objective Centric: An “Objectives Register” is the Foundation

Business at its Best:
Driving Sustainable Value Creation
Five Imperatives for Corporate CEOs

TOP VALUE CREATION OBJECTIVES
Implementing Board & C-Suite Driven/Objective Centric: An “Objectives Register” is the Foundation

The value killers revisited
A risk management study

TOP POTENTIAL VALUE EROSION OBJECTIVES
Implementing Board & C-Suite Driven/Objective Centric: Assigning Composite Residual Risk Ratings ("CRRR’s")

<table>
<thead>
<tr>
<th>COMPOSITE RESIDUAL RISK RATING DEFINITIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 Fully Acceptable – Composite residual risk status is acceptable. No changes to risk treatment strategy required at this time. (NOTE: this could mean that one or more significant risks are being accepted. Information on accepted concerns is found in the Residual Risk Status information)</td>
</tr>
<tr>
<td>1 Low – Inaction could result in very minor negative impacts. Ad hoc attention may be required to adjust composite residual risk status to an acceptable level.</td>
</tr>
<tr>
<td>2 Minor – Inaction or unacceptable terms could result in minor negative impacts. Routine management attention may be required to adjust composite residual risk status to an acceptable level.</td>
</tr>
<tr>
<td>3 Moderate - Inaction could result in or allow continuation of mid-level negative impacts. Moderate senior management effort required to adjust composite residual risk status to an acceptable level.</td>
</tr>
<tr>
<td>4 Advanced – Inaction could allow continuation of or exposure to serious negative impacts. Senior management attention required to adjust composite residual risk status.</td>
</tr>
<tr>
<td>5 Significant - Inaction could result in or allow continuation of very serious entity level negative impacts. Senior management attention urgently required to adjust composite residual risk status to an acceptable level.</td>
</tr>
<tr>
<td>6 Major - Inaction could result in or allow continuation of very major entity level negative consequences. Analysis and corrective action to adjust composite residual risk status required immediately.</td>
</tr>
<tr>
<td>7 Critical - Inaction virtually certain to result in or allow continuation of very major entity level negative consequences. Analysis and corrective action to adjust composite residual risk status required immediately.</td>
</tr>
<tr>
<td>8 Severe - Inaction virtually certain to result in or allow continuation of very severe negative impacts. Senior management/board level attention urgently required to adjust composite residual risk status.</td>
</tr>
<tr>
<td>9 Catastrophic – Inaction could result in or allow the continuation of catastrophic proportion impacts. Senior management/board level attention urgently required to adjust composite residual risk status and avert a catastrophic negative impact on the organization.</td>
</tr>
<tr>
<td>10 Terminal - The current composite residual risk status is already extremely material and negative and having disastrous impact on the organization. Immediate top priority action from the board and senior management required to prevent the demise of the entity.</td>
</tr>
</tbody>
</table>
### Risk Assessment Rigour (“RAR”) Levels

<table>
<thead>
<tr>
<th>RAR</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Assigned (NA)</td>
<td>Accountability to report on the Composite Residual Risk Rating (“CRRR”) has not been assigned to an OWNER/SPONSOR(s)</td>
</tr>
<tr>
<td>Not Rated (NR)</td>
<td>Accountability has been assigned to an OWNER/SPONSOR(s) but no CRRR has been assigned yet</td>
</tr>
<tr>
<td>Very Low (VL)</td>
<td>Accountability to report CRRR status has been assigned and a CRRR rating with a brief narrative explaining the basis for the CRRR provided by the objective OWNER/SPONSOR(s) within the past 12 months</td>
</tr>
<tr>
<td>Low (L)</td>
<td>A time-limited effort has been made to develop or update a list of risks/threats to achievement and assign RED/AMBER/GREENS to each risk within the past 12 months. Action items for all RED rated risks will be developed</td>
</tr>
<tr>
<td>Medium (M)</td>
<td>More effort has been spent to quality assure that all significant risks have been identified using a variety of risk identification methods and the risk treatments in place/use for all, or some, of the risks have been identified and documented. Performance and impact information for the objective has been obtained and documented. Data has been updated within the past 12 months.</td>
</tr>
<tr>
<td>High (H)</td>
<td>A range of techniques have been used to identify all significant risks. Risk treatments for risks have been identified and efforts made to independently validate the existence and effectiveness of the risk treatments. Efforts have been made to validate the adequacy and accuracy of the linked objective performance and impact information.</td>
</tr>
<tr>
<td>Very High (VH)</td>
<td>All standard RiskStatusline™ information elements have been identified and documented and additional efforts made by the OWNER/SPONSOR(s) to validate their completeness and reliability.</td>
</tr>
<tr>
<td>Very High + (VH+)</td>
<td>In addition to identifying and documenting all standard RiskStatusline™ data elements, more advanced techniques to determine velocity of risks, leading/lagging risk indicators, steps taken to assess the reliability of likelihood and consequence ratings and other advanced risk assessment techniques</td>
</tr>
</tbody>
</table>
Implementing Board & C-Suite Driven/Objective Centric: Transparent Independent Assurance Level (“IAL”)

NIA – No independent assurance
LOW – A high level assurance review has been completed and a feedback report provided to the OWNER/SPONSOR and RISK OVERSIGHT COMMITTEE
MEDIUM – An independent review has been completed to assess the completeness of risks identified, risk treatments and residual risk status information provided and a report provided to the OWNER/SPONSOR and RISK OVERSIGHT COMMITTEE
HIGH – In addition to the steps defined for MEDIUM, steps have been taken to confirm the existence and effectiveness of the risk treatments identified.
The Way Forward - It's Time to Self-Assess
The Way Forward – It’s Time to Self-Assess

Richard Chambers @rfchambers · Sep 8

“An internal audit operation that is performing against outdated expectations is an accident waiting to happen.”

#Audittraillesson

© Risk Oversight Solutions Inc.
The State of the Internal Audit Profession

PwC has published the 2014 edition of their State of the Internal Audit Profession.

The stated theme is bland: “alignment of stakeholder expectations, and matching skills and capabilities to those expectations, helps internal audit enhance the value delivered to the organization.”

But there is a clear message to internal audit leaders, as well as to audit committee members and others with oversight responsibility for internal audit.

About half the internal audit departments around the world are failing to deliver the assurance and advisory services their stakeholders need – and know they need.

As I reported in January, a KPMG survey of Audit Committee members found that “Fewer than half of the 1,800 respondents are satisfied that internal audit delivers the value to the company it should (45%), and that the internal audit plan properly focuses on the ‘critical risks to the enterprise’ (49%).”

Now, PwC is reporting similar results:

- “Nearly 30% of board members believe internal audit adds less than significant value”. (This is an increase from the 20% PwC reported from their 2013 survey).
- “More than half (55%) of senior management told us that they do not believe internal audit adds significant value to their organization”.
- “Even CAEs are critical of their function’s performance, with just 65% believing on average that their function is performing well”.
- Only 53% of respondents believe internal audit is focusing on the “critical risks and issues the company is facing”.

risk oversight solutions
A better response to risk.
The Way Forward – It’s Time to Self-Assess

State of ERM Maturity

25% believe their organization has a "complete formal enterprise-risk management process in place," and that finding does not differ from the prior year, suggesting that no significant strides in risk oversight maturity were made over the prior year.

- Larger companies, public companies, and financial services organizations are more likely to describe their ERM at that level – about 45%

23% describe their organization’s level of risk management maturity as “Mature” or “Robust.”

- About one-third of the larger companies, public companies, and financial services organizations describe their ERM maturity at that level.

52% indicate that their organization's risk management process is “not at all” or “minimally” viewed as a proprietary strategic tool that provides unique competitive advantage, suggesting that many organizations continue to struggle to integrate ERM and strategic planning.

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.

Source: NCSU/AICPA 2015 Report on the State of Enterprise Risk Oversight
QUESTIONS??????

Tim Leech FCPA CIA  CRMA  CFE
Risk Oversight Solutions Inc.
timleech@riskoversightsolutions.com
www.riskoversightsolutions.com