EDPACS: The EDP Audit, Control, and Security Newsletter

Risk Oversight: Is it “Broken”? What are the New Expectations?
Tim Leech

Available online: 20 Apr 2012
Abstract. Following the global financial crisis of 2008 commissions were convened around the world to study what went wrong. One of the common themes that emerged is that many of the companies at the root of the financial crisis had some combination of weak risk management and deficient board oversight of risk. Unfortunately, few of the commission, including the ones convened in the U.S., even took the time to probe or consider the role internal audit played in the periods leading up to the crisis. The widely held assumption by commission members was that the approaches used by the majority of internal audit departments are incapable of preventing the type of massive governance lapse at the root of the 2008 global crisis. This article analyzes the traditional role played by boards, senior management and internal audit function and proposes significant changes in the approach used by boards, senior executives and auditors to prevent yet another wave of trust debilitating corporate governance breakdowns.

In 2002, after a flurry of colossal accounting frauds surfaced globally, the U.S. government enacted the Sarbanes-Oxley Act (“SOX”) to try to fix the problems that U.S. politicians decided were at the root of the crisis. A key belief at the time was that holding senior management more formally accountable for accounting disclosures and related controls, and forcing external auditors to form an independent opinion on whether accounting controls are “effective,” would fix the problem. In 2008, the world suffered another corporate financial crisis that made the events leading up to SOX pale in comparison. More than a few people believe that the entire world was at risk of economic collapse in the absence of aggressive government intervention.

This time government regulators from seven of the world’s economic superpowers studied the events leading up to the crisis to see what could be learned to prevent a reoccurrence. Key conclusions of that study1 are shown below.

A central finding in the study indicated deficient senior management and board risk oversight was a major cause of the collapse—in the minds of regulators the next big corporate governance problem to be fixed.
REGULATORS FOCUS ON RISK OVERSIGHT—CAN A “SOX-LIKE” SOLUTION BE AVOIDED?

In the United States, the SEC reacted to the Senior Supervisors Group conclusions by implementing new proxy disclosures rules for all US listed companies. The new rules require companies publicly disclose the board’s responsibility for risk oversight and what the board does to oversee risks of all types, including compensation risks. In Canada, the Canadian Securities Administrators has called for significant improvements in the disclosures being made related to risk management and risk management oversight and stated “In light of ongoing international developments regarding the disclosure of risk management practices, this is an area that we will continue to monitor.” Private sector initiatives are now underway in Canada and the US to try to avoid another regulator-led, SOX-like remedy.
In December 2010 the Canadian Institute of Chartered Accountants ("CICA") issued an exposure draft on the subject of board oversight of risk. The Institute of Corporate Directors in Canada held briefings on risk oversight expectations in cities across the country. In the United States, the Committee of Sponsoring Organizations ("COSO") has reported survey results that strongly suggest there is, in fact, an expectation gap. COSO issued new guidance for directors on risk oversight and has plans to overhaul the now dated 1992 COSO Internal Control—Integrated Framework. The National Association of Corporate Directors Blue Ribbon Commission on Risk Governance issued principle-based guidance for directors in October 2009 in a report titled Balancing Risk and Reward.

**HOW DO YOU KNOW IF YOUR APPROACH TO RISK OVERSIGHT IS OK?**

Whether you agree that corporate risk oversight is an area that is indeed “broken,” or not, it is clear that governments generally, and security regulators specifically, have decided that it is, and that it needs to be fixed. At Risk Oversight Inc. we do not believe that risk management and risk oversight is “broken” in the majority of companies, but we do believe that there is a growing body of evidence that traditional approaches to corporate risk and assurance management are sub-optimal. We invite you to take a few minutes to review our analysis for boards, senior management, and internal audit to see how you measure up against the new risk oversight expectations.

This issue has taken on significantly increased importance for many boards. The Board Blog identified risk oversight as one of two “800 pound guerillas” in the room for boards in 2011. Regulatory...
in the United States and Canada are currently assessing whether new regulations in this area are warranted. The introduction to this paper lists a range of private sector initiatives currently underway to try and avoid another “SOX-like” government intervention.

In Canada, the CICA released a new exposure draft on board oversight of risk in December 2010. The exposure draft suggests that in addition to the traditional governance model described in the box shown below, boards should be playing an exponentially greater, more hands-on role in risk management and risk oversight. Risk oversight frameworks in many companies are not currently well equipped to meet, at least not in a serious and demonstrable way, the expectations spelled out for traditional governance models in the box below.

CICA Board Risk Oversight Exposure Draft (December 2010)

“According to McKinsey, traditional governance models support the notion that boards cannot and should not be involved in day-to-day risk management, but that directors should, through their risk oversight role, be able to satisfy themselves that effective risk management processes are in place and implemented”.

“The risk management system should allow management to bring to the board’s attention the company’s most material risks and assist the board in understanding and evaluating how these risks interrelate, how they may affect the company, and how these risks are being addressed by management. Directors need to have the experience, training and knowledge of the business to make a meaningful assessment of those risks.”

Traditional Approach not Enough

- Company discloses a long laundry list of risks in security filings that could potentially impact the company.
- In many companies senior management does not formally report to the board on the status of the company’s risk management framework, or the significant risks being accepted by the company. In some companies the board gets the “top ten” risks, however these are often not the company’s top 10 residual risks after considering current risk treatment strategies. Not all boards receive management’s assessment of the most significant emerging risks that could impact the company.
- There may, or may not, be a report from management to the board on compliance risk, including areas like securities regulation, U.S. Foreign Corrupt Practices Act (FCPA)/Canadian Corruption of Foreign Public Officials Act (CFPOA), tax compliance, environment, safety, and other areas that can expose companies to significant reputational and financial risk.
• In companies that have an internal audit function the board receives reports on audit plans and findings of audits completed in the year, together with control “weaknesses” the auditors identified. The percentage of the total risk universe covered by internal audit each year is usually less than 20% of the total risk universe.

• In companies that do not have an internal audit function the board sees representations made by the CEO and CFO on internal control over financial reporting and the external auditor’s report. The board may, or may not, receive formal reports from management on the current effectiveness of enterprise risk management processes or the corporation’s biggest residual risks.

• Strategic and annual plans presented to the board may, or may not, include specific information on the risks identified, management’s assessment of those risks, the risk treatments and strategies that will be used to manage those risks, and the residual risk status expected.

What Needs to Change

• Significant risk acceptance decisions (conscious and unconscious) should be elevated to the board of directors to ensure there is consensus agreement on the company’s risk appetite and demonstrable evidence of senior management and board level risk oversight. Significant emerging risks should be elevated to the board and senior management should describe how they are monitoring and treating these risks.

• In companies that have an internal audit function, internal audit should be responsible for ensuring the board receives reliable and materially complete information on the company’s residual risk status. Per the Institute of Internal Auditors standards, internal audit should annually provide the board with an independent opinion on the reliability of the company’s risk management processes. Companies that do not have an internal audit function need to have a process to identify, assess, and report significant residual risks to the board.

• Strategic and annual plans presented to the board for approval should include a full discussion of the risks involved and the strategies/risk treatments in place or planned to address them.

As a direct result of the overwhelming pressure being exerted on boards to increase the quality of risk oversight many boards are taking aggressive steps and making specific requests to senior management concerning risk management and oversight.

In Canada, securities regulators have indicated that they are unhappy with the quality of public disclosures related to risk management and oversight. Although Canadian regulators have not required companies found to be deficient in 2010 to restate filings, they have demanded improvements and indicated that will be monitoring this area very closely in 2011.

A COSO 2010 study reported: “The state of ERM appears to be relatively immature. Only 28 percent of respondents describe their current stage of ERM implementation as ‘systematic, robust and repeatable’ with regular reporting to the board. Almost 60 percent of respondents say their risk tracking is mostly informal and ad hoc or only tracked within individual silos or categories as opposed to enterprise-wide.”
Traditional Approach not Enough

- Senior management in the majority of companies does not receive a consolidated report on the company’s most significant residual/retained risks. Risk information is reported from a range of sources but rarely using consistent terminology and a standardized impact rating system.

- In companies that have an internal audit function senior management usually receive a copy of the annual audit plan and results of audits conducted during the year. Although this is slowly changing, only a small percentage of internal audit departments currently provide reports on the maturity and effectiveness of the company’s risk management framework. Only a small percentage of audit departments complete their work using generally accepted risk assessment methods (e.g., ISO 31000) and provide business units with copies of the risk assessments completed, if any, by the audit team. The internal audit function is quite often the only function that completes documented risk/control assessments on a regular basis.

- In companies that do not have an internal audit function, senior management often do not require formal reports on residual risk status from business units. Only a relatively small percentage of companies have adopted a common risk vocabulary and assessment framework.

What Needs to Change

- CEOs and CFOs need to play a lead role ensuring that their company has an effective risk management framework in place.
capable of identifying and reporting upward significant residual risk acceptance decisions and emerging risks on a timely basis. Robust risk self-assessment systems need to be implemented and steps taken to ensure they are producing reliable information.

- CEOs and CFOs should receive reports on the current maturity and capability of their company’s risk management framework relative to other public companies.
- Senior management should play a lead role selecting a risk management methodology and terminology for use by work units and assurance specialist groups and leading ERM implementation efforts. ISO 31000 is gaining significant traction globally and has been recommended for use by the Institute of Internal Auditors when assessing and reporting on risk management processes.
- A key goal should be to ensure that the board is aware of, and agrees with, significant risk acceptance decisions made by the senior management team.

Ernst & Young’s 2010 internal survey, Unlock the Value of Internal Audit, noted that only 44% of respondents believe Internal Audit was helping the company achieve its business objectives. Of respondents, 96% indicated that they needed to make improvements to their Internal Audit function within the next 24 months.

In addition to the EY survey there is significant support for stakeholder’s concern that traditional internal audit is not meeting stakeholder needs. Many small to midcap public companies elect not to have an internal audit function on the premise it would not add sufficient value to justify the cost and could distract management from its core purpose of value creation. Many companies

Richard Chambers, IIA’s President and CEO, on Internal Audit Profession Outlook:

While I am encouraged by the outlook for our profession in 2011, I have to sound an important note of caution. I have seen at least two surveys recently on internal auditing’s stakeholders (management officials and board members) that may be signaling “storm clouds” on the horizon. In both surveys, respondents shared the view that internal auditing needed to “step up its game.”

Stakeholders seem to be signaling a concern that internal auditing is not adding as much value as it should. On the part of a growing number of stakeholders, there seems to be an underlying mood that while internal auditing’s focus is shifting, it is not changing fast enough. Others appear to be frustrated by the heavy emphasis on assurance and the lack of knowledge of the company’s business/industry.

have an internal audit function because they have been told they should. Fearing high costs and inadequate return on investment, some NYSE listed companies have elected not to implement an Internal Audit function in spite of being required to do so by the NYSE Governance code. Clearly there is a serious expectation and value gap that needs to be addressed.

**Traditional Approach not Enough**

- Traditional internal audit methods do not provide robust support for boards and senior management that want to demonstrate effective risk oversight.
- Traditional internal audit planning processes tend to be process/control centric. They have not done well identifying significant value eroding retained risks that impact share value (e.g., 2008 financial crisis, stock option backdating and others).
- Traditional audits identify what the audit team believe are significant/notable control weaknesses. Coverage of the total risk universe each year is usually less than 20%. Few audit departments use a generally accepted risk assessment framework and consistent risk management terminology, and few audit functions report to the board and senior management on the areas that have not been audited or reported on during the year that could significantly impact the company.
- Audits provide information on control weaknesses in areas assessed but do not provide much orientation to work units on how to formally assess and report on risk. Few internal audit departments turn over their risk assessments to work units for the work unit to maintain and update going forward.
- Only a small percentage of internal audit departments currently provide formal reports on the organization’s risk management processes relative to other companies, or the company’s consolidated residual risk position.

**What Needs to Change**

- Internal audit should focus on identifying the company’s current residual risk status and elevating significant residual risk acceptance decisions for review by senior management and the board. Although traditional audit approaches result in audit deciding what areas have “control deficiencies” or “areas needing improvement”, this is not optimal. Internal audit’s primary job should be to ensure senior management and the board are aware of the company’s current residual risk status and the significant risks being accepted.
- Measuring internal audit’s performance on how well it completes their audit plan, a metric still used by many internal audit departments, should be replaced with metrics linked to outcomes that add real value. We believe that the most important performance metrics for internal audit should be whether senior management and the board are aware of the most significant risks being accepted across the enterprise, and the contribution internal audit has made towards improving the company’s risk management capability.
Internal audit functions should select and use an assessment approach linked to internationally accepted risk management standards for all of their assessment and reporting activities and promote the use of consistent risk terminology across the enterprise.

Two decades ago, in 1990, Tim Leech, Managing Director Global Services Risk Oversight Inc., wrote "boards of directors, officers, managers, and auditors that use the ‘historical/traditional approach’ to control and risk management should be dissatisfied and actively searching for a more effective replacement."[13]

Unfortunately for investors and public companies around the world the traditional approach to risk governance has proven to be amazingly resilient in spite of its deficiencies and numerous high profile failures. Risk oversight expectations for boards and senior management appear to still be in the “good/best practice” category as opposed to a defined legal duty of care. Prudent companies are not waiting to see if this will change going forward. Not reacting heightens the risk of another SOX-like solution.

Risk Oversight Needs to Improve

- More than a decade after the Saucier Committee report[14] referenced at right in Canada, and more than 8 years after the first NACD Blue Ribbon Commission on risk oversight[15] in the United States, an ERM survey conducted by COSO reported that “Almost 60 percent of respondents say their risk tracking is mostly informal and ad hoc or only tracked within individual silos or categories as opposed to enterprise-wide.”[16]
- The same December 2010 COSO survey reported that “More than half of the survey participants noted the board’s risk oversight process is either ‘effective’ or ‘highly effective,’ however, there also is general agreement that there should be a more structured process.”
- There is growing evidence that companies that want to avoid severe reputation damage to the company, its board, and senior management need to implement more demonstrable risk management processes that meet the type of broad criteria defined in the sidebar to the right.
- Our observations and recent survey results suggest that only a minority of public companies today have robust processes capable of demonstrating all four attributes of an effective risk management system defined by WLRK, shown below.

What Needs to Change

- Organizations need to take a formal inventory of their current risk management processes.
- Boards and senior management need to research and jointly agree on a target level of risk management maturity.
- The target level of risk management maturity needs to be compared to the current maturity and a plan developed to close gaps over an agreed timeframe (a “Risk Management Maturity Gap Assessment”).
In December 2010, Wachtell, Lipton, Rosen & Katz ("WLRK"), a US law firm, issued an advisory on risk oversight expectations which proposes some specific criteria for "effective" risk oversight drawing on emerging US law and regulation:

*Risk management should be tailored to the specific company, but in general an effective risk management system will:*

1) *Adequately identify the material risks that the company faces in a timely manner;*

2) *Implement appropriate risk management strategies that are responsive to the company’s risk profile, business strategies, specific material risk exposures and risk tolerance thresholds;*

3) *Integrate consideration of risk and risk management into business decision-making throughout the company; and*

4) *Adequately transmit necessary information with respect to material risks to senior executives and, as appropriate, to the board or relevant committees.*

- The “adequacy” of the current risk governance framework should be assessed by independent specialists using the new Institute of Internal Auditors IPPF Practice Guide *Assessing the Adequacy of Risk Management Using ISO 31000* issued in December 2010, or other suitable criteria that the board of directors and management consider valid.

**Notes**

Tim Leech, FCA, CIA, CFE, CCSA, is Managing Director Global Services at Risk Oversight Inc. and one of RO’s founding partners; he has more than 25 years global experience helping company boards, senior management/workgroups, internal auditors and other assurance specialists implement more cost effective risk management and risk oversight frameworks (tim.leech@riskoversight.ca). Risk Oversight Inc. was established in October 2010 to help companies, directors, internal auditors, and risk specialists meet new and emerging risk oversight expectations in the United States and Canada. The company has offices in Calgary, Alberta, Oakville, Ontario, and Bethlehem, Pennsylvania.