The Future Role of Internal Audit in (Enterprise) Risk Management

John Shortreed, Ph.D.
Professor Emeritus, University of Waterloo, Canada
www.irr-neram.ca

John Fraser
Senior VP, Internal Audit and Chief Risk Officer, Hydro One, Ontario, Canada,
www.hydroone.com

Grant Purdy
Associate Director, Broadleaf Capital International,
Immediate past chair Standards Australia
and Standards New Zealand risk management committee, Head of delegation to ISO PC 262 – risk management
http://www.broadleaf.com.au

Arnold Schanfield, CIA, CPA
Director of the Education and Research Center For Managing Risk,
Manhattanville College

arnold.schanfield@mville.edu

1.0 Introduction

Internal audit is at a cross roads and will in the next couple of years need to modify its traditional approaches, tools and techniques to meet new legislative requirements for corporate governance and new risk management standards. These new requirements are designed to provide better assurance of an organisation's capability to manage risk that will require major changes in internal audit practice and support for that function by the board.

Economic and social catastrophies such as: Enron, the 2008 banking crisis, Katrina, BP, Olympus, Greece, etc., have happened too frequently. Such catastrophes resulted from poor governance in both private and/or public orgainzations. Governance failures can be attributed in large part to inadequate risk management (including ineffective monitoring by internal audit).

International guidelines for the management of risk were standardized in ISO 31000:2009, Risk management: Principles and guidelines. This standard provides an up to date and practical guide for all organizations, private or public, to improve and enhance their ability to manage risk. It is based on earlier risk management standards and the practical successes of organizations using such techniques, such as Hydro One and BHP Billiton. Hydro One implemented ERM, an earlier version of ISO 31000, starting in 2000 using the AS/NZS 4360 risk management standard as their template. Their successes and challenges in managing their risks have been well documented (Simkins 2004, Mikes 2008 and 2009). Their model which is based primarily on the use of risk workshops, prioritization of risks and the allocation of resources, has operated on a simple but effective facilitation model. The Chief Audit Executive has separate audit and risk management staff and wears two different hats in accordance with

the Institute of Internal Auditors approved method of involvement of internal audit with ERM (IIA 2004 and 2011). The Hydro One model determines the highest sources of risks and presents them to senior management and the board for review and treatment. Risk criteria are established and agreed at the board level as the basis for identifying, analysing and evaluating risks. Internal audit uses this risk profile, in an exemplary way, as the high level basis for their internal audit planning.

Recently, many of the major countries have introduced regulations and codes that address Corporate Governance (for example King III in South Africa, Combined Code in UK and ASX in Australia). These all require that an organization's Board is provided with sufficient information that it can attest to shareholders that effective risk management is taking place or to disclose deficiencies if this is not the case. Typically these regulations and codes require Boards to disclose: (Canadian Securities Administrators, 2010)

- Information about the issuer's risk profile and its most significant risks;
- Advice on how the management of risk has been integrated into the organization's other important business processes and, in particular, into strategic management;
- The organization's policy with respect to the management of risk; and
- The board's assessment of the effectiveness of risk management policies and procedures, including its risk management framework and process.

These changes require an appropriate response from the internal audit profession, including:

1. to play a role in the management of risk and not just provide an independent view of management's efforts;
2. to support risk management by providing assurance on critical controls;
3. to develop new techniques for monitoring, review, and communication, to improve the effectiveness of both risk management and governance in their organizations; and
4. in cooperation with their colleagues around the world to change the requirements, training and practice of internal auditors to meet these innovative, expanded and important challenges.

It goes without saying that these new roles for internal audit as well as traditional roles must be monitored to ensure performance meets expectations. Also to give assurance to stakeholders, a key requirement of ISO 31000, it will be necessary to have explicit approaches for internal and external communications. ISO 31000 provides guidence on this.

This paper explores the new governance requirements, the latest standards for risk management and the implications for internal audit. The main conclusions of the paper are shown in italics in the text as they are developed.

2.0 Risk Management and Organizations – Recent trends

There are a number of recent developments and trends concerning both the concept of risk and the general arrangements for its management in organizations that have a significant impact on internal audit activities.

2.1 Taking risk is beneficial.

Risk is now considered to be "*the effect of uncertainty on objectives*" (ISO 2009). Risk can be characterized by either or both, positive and negative consequences. These consequences must be linked to the objectives of the organization. For example, beneficial outcomes might be an improvement in customer satisfaction with goods or services as a result of 'controls' ("*measure that is modifying risk"*) such as focus groups about new goods or services. These controls will increase the likelihood of better outcomes. *Conclusion 1 Risk management concerns reducing the magnitude and likelihood of detrimental consequences while enhancing and making more likely the beneficial consequences that might arise from decisions.*

2.2 The organisation's ability and capability to manage risk and not just controls should be the focus of internal audits.

This is illustrated by a suggestion that the Sarbanes Oxley Act in the USA should be revised so that the focus of audit moves from controls to risk management (Leech, 2011). The reason given for this is that the failures of organizations in the 2008 banking crisis, and other recent financial failures, were not so much the failure of existing controls, but rather the lack of appropriate controls due to the failure to effectively identify, analyse, evaluate and therefore treat risks. *Conclusion 2 The focus of internal audit and other monitoring and review functions should be to provide assurance on the effectiveness of risk management not just on the effectiveness of controls.* The management of risk should always be understood to be concerned with the achievement of the organisation's objectives. Controls are then just 'enablers for those objectives' and while they are the sharp edge of the risk management process they are only as good as that process. Internal audits of risk management should also form the basis for the organization's overall assessment of their risk management which in turn is the starting point for any external review of their risk management as well as for external communications about risk.

2.3 Risk management requires a clear and sustained intent from management.

Risk management should be fully integrated with the strategic planning and other management processes. Because risks are the effect of uncertainty on objectives, the setting of subordinate objectives (for example for business plans, programs and projects) must also incorporate risk management. This is because: (International Corporate Governance Network, 2010)

> "risk taking is an inseparable element of strategy and a crucial driver in achieving objectives, …. Risk is part of every decision a company makes. Strategy and risk are not new concepts, although it is recognised that risk is a subject of increasing attention and regulatory and legislative movements in many jurisdictions. The …ability to gauge and respond to how a company is managing risk has broader relevance beyond the board and shareholders alone. It bears on the company's impact on all stakeholders including employees and the communities in which an enterprise does business, and in certain instances, national or international markets"

In the opinion of the authors, addressing "impact on all stakeholders" is a key requirement for success in today's world with its instanteneous social communications and their impacts on organizations. The "Brent Spar" saga where Shell could not do the right thing for the environment due to inadequate communication with stakeholders is a cautionary tale, including the unusual recanting by Greenpeace of of their advice because of errors. (Wikipedia, Brent Spar)

In reviewing the 2008 banking crisis, a number of failures of risk management were identified as having occurred that are applicable to many other organizations (Financial Stability Board, 2009**):**

- the unwillingness or inability of boards of directors and senior managers to articulate, measure, and adhere to a level of risk acceptable to the organization, …. often there was a disparity between the risks taken and those that their boards perceived the organization to be taking;
- internal arrangements including management compensation that conflicted with or were misaligned with the objectives of the organization; and
- an inadequate and often fragmented infrastructure that hindered effective risk identification, analysis, evaluation and treatment.

Conclusion 3 Processes for the management of risk must be integrated into an organisation's systems of management to be effective. While the recent trends have been directed at risk management activities to generate governance reports, for these to be meaningful and reliable, this requires that consistent and comprehensive risk management be applied throughout the organization, including suitable contributions from assurance providers such as internal auditors. In response to recent failures, focus has been on improving the governance of organizations and those improvements have largely been a call for "more effective risk management".

3.0 ISO 31000:2009, Risk management – Principles and guidelines

ISO 31000 reflects current best practise. It was developed through a four-year process that involved many thousands of risk management practitioners from around the world in the development of a consensus document. It contains advice on how a framework for risk management can be implemented and enhanced. It was developed in an era where there were many competing frameworks, COSO (2004), project management standards, COBIT, etc. However, unlike those other standards, the ISO standard is not specific to any country, application or type of risk. It is a forward-looking document that reflects the characteristics of best practise in leading organizations. For example, the mining industry and the resource sector in general require very effective risk management to generate returns on investments, to protect their 'licence to operate' and to provide good standards of safety for their employees and neighbouring communities. The biggest mining firm in the world is BHP Billiton and its risk management policy (circa 2007) is shown in Figure 1. It illustrates virtually all the key attributes of best practise in risk management that are included in ISO 31000. In this section the key innovations in ISO 31000 are presented along with implications for internal audit.

3.1 Risk management is integrated into the organization's systems of management and decision-making

> "Organizations develop, implement and continuously improve a framework whose purpose is to integrate the process for managing risk into the organization's overall governance, strategy and planning, management, reporting processes, policies, values and culture" (ISO, 2009).

Every risk should have a designated risk owner, who provides leadership for addressing the risk and makes the decisions for that risk; i.e. risks are "owned" by the decision maker and not by a separate group such as internal audit or the risk management department. This is one of the most important innovations in ISO 31000 – risk management is fully integrated into the command, control, and reporting structure of the organization and is not a stand-alone activity.

Every organization according to its mandate, vision, and objectives organizes a corporate structure to meet its mandate and achieve its objectives. Organization charts are one expression of this organizational structure. ISO 31000 maintains that the management of risk is just one consideration among many used by each individual manager in the organization when making decisions. In supporting decision-making, risk management joins other key decision-making inputs, as for example: human resources, budgeting, execution of assigned work tasks, and current ethical policies. Risk management is implemented to ensure that uncertainties associated with decisions are identified, analysed, evaluated, treated and monitored leading to enduring controls. *Conclusion 4 Internal Audit should no longer assess risks on behalf of the organisation. Their role is to assist decision-makers in arriving at the most appropriate treatment of risks and then the monitoring and review of risks and controls.* The term "assess risks" in this paper means meeting the criteria and guidelines for risk assessment given in ISO 31000. This is because assess is part of management's job and not internal audit's.

Conclusions 2 and 4 mean that the traditional internal audit practice of assessing risks is no longer required. Indeed it is undesirable as it reduces the accountability of management. The risk assessment done by internal audit has traditionally been focused on the design of an audit plan rather than to support decision-making. Figure 2, shows the ISO risk management process to be used by all decision-makers (ISO 31000, 2009). In Figure 2 the output of the risk assessment process by the risk owner can be used directly as the starting point for an internal audit and in the development of the annual internal audit plan. Also in Figure 2 another output of the risk management process is a risk treatment plan that includes, according to ISO 31000:

- "the reasons for selection of treatment options, including expected benefits to be gained;
- those who are accountable for approving the plan and those responsible for implementing the plan;
- proposed actions;
- resource requirements including contingencies;
- performance measures and constraints;
- reporting and monitoring requirements; and
- timing and schedule."

Thus the risk management process used by the decision-maker yields all the basic inputs needed for the planning of internal audits. The Joint Institute of Internal Auditors Research Foundation, Standards Australia handbook on 'Delivering Assurance' recognizes this explicitly (Standards Australia, 2010). *Conclusion 5 Internal audit will obtain planning information for an audit (and for their annual audit plans) from the risk management process done by decision-makers who own and are accountable for the risks.*

It is not clear how quickly internal audit will adapt to these changes, from traditional roles, to this new "support the risk owner/decision-maker" role. However, it is clear that their basic function of providing an independent, reliable, unbiased monitoring and review of risks, risk management and controls is unchanged. Many new techniques will need to be tried and evaluated.

3.2 Framework for Managing Risk

ISO 31000 suggests that organisations need a clear framework and system of management that describes how they will provide suitable capability to match their intent to manage risk. The key process in managing risk is illustrated in Figure 2. (ISO, 2009). This process is used by every decision-maker for every decision. The risk management framework of 31000 exists primarily to ensure that this process is used and is effective.

The risk management framework described in ISO 31000 is based on continuous improvement by means of the traditional Plan-Do-Check-Act (PDCA) process (Deeming, 1986). A recent best selling university textbook on Enterprise Risk Management (Fraser, 2010) has characterized the essential practical elements of ERM. It is clear that ERM and ISO 31000 risk management frameworks are the same thing with the later being the principles and guidelines and the former the practical application. It is expected that the implementation of the ISO guidelines for the risk management framework will evolve in cooperation with ongoing initiatives in ERM. *Conclusion 6 ERM and the ISO 31000 risk management standard have evolved cooperatively and will be the basis for risk management in organizations*.

Figure 3 (CSA, 2011) illustrates a typical risk management framework for an organization and includes typical committees and activities involved in implementing the framework and also in continuously improving the framework. This figure originated with Broadleaf Capital International (Broadleaf, 2008) and Canadian Standards Association (CSA) in their risk management standard expanded the figure by adding the link to the organization's governance.

In Figure 3, the "review and improve" box in the lower left contains the traditional internal audit function of "control assurance", along with other reviews of governance, risk management maturity, and progress in implementing the framework. These reviews then feed into the upper left box of "mandate and commitment" leading to a cycle of continuous improvement.

In Figure 3, the framework supports the application of the 'central' risk management process. The figure identifies that training is required to implement the framework, the board's risk management committee, and other activities and committees to implement and continuously improve the framework. Figure 3 also shows a key element in ERM – the commitment and mandate for risk management from the organization's governance functions. *Conclusion 7 Effective risk management requires clear expressions of intent and mandate by the Board and*

top management. This requirement is emphasised in the Canadian risk management standards, which adds this as a basic principle as well as illustrating practical methods of expressing this commitment (CSA, 2011). Figure 1 also illustrates how the organization's risk management policy expresses both mandate and commitment.

3.3 ISO 31000 introduces the concept of "establishing the context" in relation to the design of the risk management framework

Context is established by "*defining the external and internal parameters to be taken into account when managing risk, and setting the scope and risk criteria for the risk management policy*". This step in the design of the framework is critical to ensure that the framework, which will be different for each organization, is compatible with the organization's environment, risk profile, history, and so forth. For example, a public organization which is subject to political oversight and has historically experienced rapid shifts in policy directions will want a risk management framework that recognizes the need to have both transparency but also to ensure they do not get "painted into a corner" when making decisions.

Unlike other ISO standards, ISO 31000 is written explicitly to preclude its use for certification. This is because the risk management framework must be tailored to the organization's context to be effective and every organisation is and must be different. While the main elements of the framework will be recognizable between organizations, they will be different as they are integrated into each organisation's specific systems of management.

Organizations have many existing risk management processes for: health and safety regulations, employment standards, legal precedence, and so forth. All organisations already manage risk and therefore have in place an existing, but often 'ad hoc', risk management framework. However, this is unlikely to be fully effective and ISO 31000 allows for the review of these existing approaches when enhancements are planned. One objective of ISO 31000 is to provide a standard for the harmonisation of all other standards that deal with the management of risk so that they become consistent and aligned with, ISO 31000. *Conclusion 8 Evolutionary modifications to the role and practise of internal audit will occur as part of continuous improvement of the framework for the management of risk.* It usually takes at least 3 to 5 years to implement effective risk management in an organization and during this period of time the continuous improvement process will update and mature the framework. This will include enhancing and changing the roles of internal audit and other staff functions in the organization. This provides for an orderly and effectiveness-driven modification of existing processes critical to risk management.

3.4 Risk Management Maturity While ISO 31000 provides basic principles that ERM should meet, it also (in Annex A) provides five attributes for "excellence" in risk management (ISO, 2009) and these attributes are:

1. **"Continual improvement** through the setting of organizational performance goals, measurement, review and the subsequent modification of processes, systems, resources, capability and skills.
2. **Full accountability for risks,** controls and risk treatment tasks. Designated individuals fully accept accountability, are appropriately skilled and have adequate resources to

check controls, monitor risks, improve controls and communicate effectively about risks and their management to external and internal stakeholders

3. **Application of risk management in all decision making**, whatever the level of importance and significance, involves the explicit consideration of risks and the application of risk management to some appropriate degree.
4. **Continual communications** with external and internal stakeholders, including comprehensive and frequent reporting of risk management performance, as part of good governance.
5. **Full integration in the organization's governance structure** is viewed as central to the organization's management processes, such that risks are considered in terms of effect of uncertainty on objectives. The governance structure and process are based on the management of risk. Effective risk management is regarded by managers as essential for the achievement of the organization's objectives".

ISO 31000 also indicates how risk management performance can be evaluated against these measures. This is usually done on at least an annual basis under the title of "Risk Management Maturity Evaluation". For example in Canada, Frazer Valley Health who operate 3 hospitals, conducts an annual evaluation of some 21 attributes of risk maturity to ensure that the implementation of ERM is proceeding and being continuously improved (Parkins, 2009). The basic methodology and requirements are derived from Accreditation Canada, a federal regulator. This system for auditing risk management in health care has been in place for at least a decade prior to ISO 31000 and is a good example of best practise in risk management that provided the basis for ISO 31000.

Conclusion 9 the maturity of risk management should be evaluated and reported on at least an annual basis. While this measurement of risk maturity is best undertaken by management, its verification is clearly a role for internal audit.

4.0 Evolving Roles for Internal Audit

The charter for the Royal Bank of Canada's board audit committee states, "The Committee shall annually review and assess the adequacy of its mandate and its effectiveness". While directed at the board's audit committee this mandate should also apply to its key resource, namely the internal audit function, which should also annually review and assess the adequacy of its mandate and effectiveness. The potential for evolution of internal audit into a more strategic function has been documented in a case study by Chada, (2011). She argues that in the post-ERM world internal audit will have to innovate and grow their function, moving from control and compliance monitoring to develop two new roles:

1) to provide high quality, relevant business insights, and
2) to become a subject matter specialist to management around strategic initiatives, challenges and changes in the organization.

She argues that internal audit has the people, knowledge and experience to effectively provide these two new functions.

Conclusion 10 Internal Audit has to update its roles and responsibilities to support continuous improvement of and implementation of more effective risk management Chada (2011) suggests 6 questions to start strategic planning for the new roles for internal audit:

1) Does your Internal Audit function know the expectations of its stakeholders?
2) Are the goals of your Internal Audit function aligned with those of your organization?
3) Does your Internal Audit function have a reasonable balance between assurance and advisory work?
4) Does your Internal Audit function have the right staffing mix to provide the advice and expertise your organization seeks?
5) Do you need to redefine the mandate for your Internal Audit function?
6) Is your Internal Audit function a pipeline for organizational leadership?

The issue of the linkage and alignment of internal audits and external audits is a good example of the many issues to be resolved in the evolving roles of internal audit. For providing assurance to stakeholders, external audits are needed. In the view of the authors, external audits are likely to start with the results of internal audits of the organization's overall risk management. However, the content of the internal audits will stay internal similar to assurance concerning financial integrity, with separate internal and external monitoring and reviewing. 31000 requires organizations to "tailor" their risk management framework to their context, structure, and roles and responsibilities. Each organization is unique and the risk management framework and policy will also be unique and driven by the organization's policies on what it wishes to communicate to external stakeholders, over and above what is required by regulations.

5.0 Conclusions

New Corporate Governance requirements that require Boards to gain assurance as to the effectiveness of risk management as well as the publication by ISO of an international consensus standard on the principles and guidelines for effective risk management, have created challenges and opportunities for traditional internal audit. Over the next few years internal audit will have to change its role and approach to enhance its support for effective risk management.

It is concluded that:

1. Risk management concerns reducing the magnitude and likelihood of detrimental consequences while enhancing and making more likely the beneficial consequences that might arise from decisions.
2. The focus of internal audit and other monitoring and review functions should be to provide assurance on the effectiveness of risk management and not just on the effectiveness of controls.

3. Processes for the management of risk must be integrated into an organisation's system of management to be effective.
4. Internal Audit should no longer assess risks on behalf of the organisation. Their role is to assist decision-makers in arriving at the most appropriate treatment of risks and then the monitoring and review of risks and controls.
5. Internal audit will obtain planning information for an audit (and for their annual audit plans) from the risk management process done by decision-makers who own and are accountable for the risks.
6. ERM and the ISO 31000 risk management standard have evolved cooperatively and will be the basis for risk management in organizations.
7. Effective risk management requires clear expressions of intent and mandate by the Board and top management.
8. Evolutionary modifications to the role and practice of internal audit will occur as part of continuous improvement of the framework for the management of risk.
9. The maturity of risk management should be evaluated and reported on at least an annual basis.
10. Internal Audit has to update its roles and responsibilities to support continuous improvement of and implementation of more effective risk management.

References

Aabo, T., J.R.S. Fraser, and B.J. Simkins, 2005, "*The Rise and Evolution of the Chief Risk Officer: Enterprise Risk Management at Hydro One*", Journal of Applied Corporate Finance, 17 (3), 62-75.

Australia Securities Exchange (ASX) Corporate Governance Council, 2007, *Corporate Governance Principles and Recommendations, 2nd Edition*, http://asx.ice4.interactiveinvestor.com.au

Broadleaf Capital International, 2008, home page, www.broadleaf.com.au

CSA (Canadian Standards Association), 2011, *CSA Q31001-11,Implementation guide to CAN/CSA-ISO 31000, Risk management – Principles and guidelines*, Toronto

Canadian Securities Administrators (CSA), December 2010, *Staff Notice 58-306 2010 Corporate Governance Disclosure Compliance Review* http://www.osc.gov.on.ca/documents/en/Securities-Category5/csa_20101203_58-306_2010-corp-gov-disclosure.pdf

COSO, (Committee of Sponsoring Organizations of the Treadway Commission), 2004, *Enterprise Risk Management — Integrated Framework (2004)*,

Chada, Monica, 2011, *Developing a Strategic Plan for Your Audit Function*, Annual conference of Canadian Internal Audit Association, Toronto

Deming, W.E., 1986, *Out of the Crisis*, MIT Press

Financial stability board, 2009 *Risk Management Lessons from the Global Banking Crisis of 2008* – http://www.financialstabilityboard.org/publications/r_0910a.pdf

Fraser, John and Betty Simkins, Eds., 2010, *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives*, Toronto, Wiley

Institute of Internal Auditors, 2004, *The Role of Internal Auditing in Enterprise-wide Risk Management*

Institute of Internal Auditors Research Foundation IIARF, March, 2011, White Paper, *Internal Auditing's Role in Risk Management*

International Corporate Governance Network, 2010, *ICGN Corporate Risk Oversight Guidelines*
http://www.icgn.org/files/icgn_main/pdfs/best_practice/icgn_cro_guidelines_(short).pdf

ISO (International Organization for Standardization, 2009 *ISO31000 Risk Management: Principles and Guidelines*

Leech, Tim, and Leech L., 2011, *Preventing the Next Wave of Unreliable Financial Reporting: Why U.S. Congress Should Amend Section 404 of the Sarbanes-Oxley Act*, Risk Oversight Ltd., http://riskoversight.ca/

Mikes, Anette, 2008 ,"*Enterprise Risk Management at Hydro One*", Harvard Business School Case Study 9-109-001

Mikes, Anette, 2009, "*Enterprise Risk Management at Hydro One*", Harvard Business School Multimedia/Video Case Study 110-707

Parkins, Sandra, 2009, *ERM Readiness Assessment Tool*, Conference Board of Canada.

Standards Australia, 2010, *Delivering Assurance based on ISO 31000:2009 Risk management – principles and guidelines, HB 158:2010, Standards Australia, The IIA Research Foundation, The Institute of Internal Auditors Australia, ISBN 978 0 7337 9489 6, http://infostore.saiglobal.com/store/Details.aspx?ProductID=1396045, Sydney*

Wikipedia, ongoing, *Brent Spar (a comprehensive and balanced documentation of the situation and the actions of Shell, the media and Greenpeace). http://en.wikipedia.org/wiki/Brent_Spar*

Figure 1 BHP Billiton Risk Management Policy Statement (BHP Billiton web site, 2007) (underline added to highlight key innovations of ISO 31000)

Risk is inherent in our business. The identification and management of risk is central to delivering on the Corporate Objective.

- By understanding and managing risk we provide greater certainty and confidence for our shareholders, employees, customers and suppliers, and for the communities in which we operate.
- Successful risk management can be a source of competitive advantage.
- Risks faced by the Group shall be managed on an enterprise-wide basis.
- Risk Management will be embedded into our critical business activities, functions and processes. Risk understanding and our tolerance for risk will be key considerations in our decision making.
- Risk issues will be identified, analysed and ranked in a consistent manner. Common systems and methodologies will be usedRisk controls will be designed and implemented to reasonably assure the achievement of our Corporate Objective. The effectiveness of these controls will be systematically reviewed and, where necessary, improved.
- Risk management performance will be monitored, reviewed and reported. Oversight of the effectiveness of our risk management processes will provide assurance to executive management, the Board and shareholders.
- The effective management of risk is vital to the continued growth and success of our Group.

signed Chip Goodyear **Chief Executive Officer**

Figure 2 – Risk Management Process (ISO, 2009)

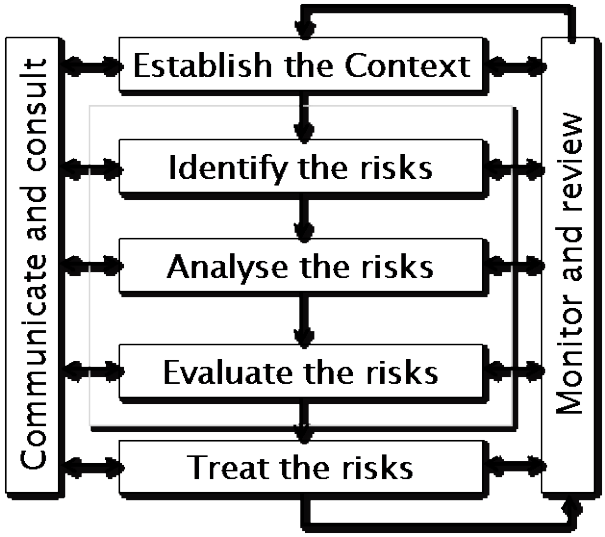

Figure 3 Example of an ERM framework for a typical larger organization.
(CSA, 2011)