The Institute of Internal Auditors

September 29, 2004

The Role of Internal Auditing in Enterprise-wide Risk Management

In conjunction with the newly released Committee of Sponsoring Organizations of the Treadway Commission (COSO) *Enterprise Risk Management - Integrated Framework*, The Institute of Internal Auditors (IIA), in coordination with its IIA-UK and Ireland affiliate, has issued a position paper on *The Role of Internal Audit in Enterprise-wide Risk Management*. The paper's purpose is to assist chief audit executives (CAEs) in responding to enterprise risk management (ERM) issues in their organizations. The paper suggests ways for internal auditors to maintain the objectivity and independence required by The IIA's *International Standards for the Professional Practice of Internal Auditing* (*Standards*) when providing assurance and consulting services.

Internal auditing's core role with regard to ERM is to provide objective assurance to the board on the effectiveness of an organization's ERM activities to help ensure key business risks are being managed appropriately and that the system of internal control is operating effectively

Recommended Roles

The main factors CAEs should take into account when determining internal auditing's role are whether the activity raises any threats to the internal auditors' independence and objectivity, and whether it is likely to improve the organization's risk management, control, and governance processes. The IIA's position paper indicates which roles internal auditing should and should not play throughout the ERM process.

Core internal auditing roles in regard to ERM.

- Giving assurance on risk management processes.
- Giving assurance that risks are correctly evaluated.
- Evaluating risk management processes.
- Evaluating the reporting of key risks.
- Reviewing the management of key risks.

Legitimate internal auditing roles with safeguards.

- Facilitating identification and evaluation of risks.
- Coaching management in responding to risks.
- Coordinating ERM activities.
- Consolidating the reporting on risks.
- Maintaining and developing the ERM framework.
- Championing establishment of ERM.
- Developing risk management strategy for board approval.

Global Headquarters
247 Maitland Avenue
Altamonte Springs, FL
32701-4201 USA
Tel: +1-407-937-1100
Fax: +1-407-937-1101
www.theiia.org

Roles internal auditing should NOT undertake.

- Setting the risk appetite.
- Imposing risk management processes.
- Management assurance on risks.
- Taking decisions on risk responses.
- Implementing risk responses on management's behalf.
- Accountability for risk management.

The Institute emphasizes that organizations should fully understand that management remains responsible for risk management. Internal auditors should provide advice, and challenge or support management's decisions on risk, as opposed to making risk management decisions. The nature of internal auditing's responsibilities should be documented in the audit charter and approved by the audit committee.

Finally, *The Role of Internal Audit in Enterprise-wide Risk Management* is attached.

Established in 1941, The IIA serves approximately 95,000 members in internal auditing, governance, internal control, IT audit, education, and security worldwide. The Institute is the recognized authority, principal educator, and acknowledged leader in certification, research, and technological guidance for the profession worldwide.

Position Statement

The Institute of Internal Auditors

The Role of Internal Audit in Enterprise-wide Risk Management

Introduction

Over the last few years, the importance to strong corporate governance of managing risk has been increasingly acknowledged. Organisations are under pressure to identify all the business risks they face; social, ethical and environmental as well as financial and operational, and to explain how they manage them to an acceptable level. Meanwhile, the use of enterprise-wide risk management frameworks has expanded, as organisations recognise their advantages over less coordinated approaches to risk management.

Internal audit, in both its assurance and its consulting roles, contributes to the management of risk in a variety of ways. In 2002 The Institute of Internal Auditors – UK and Ireland issued a position statement on *The Role of Internal Audit in Risk Management* to provide guidance to members on the roles that were permissible and the safeguards needed to protect internal audit's independence and objectivity. This new revised position statement supersedes the earlier one and takes account of recent developments from around the world in the field of risk management and in internal audit.

What is Enterprise-wide Risk Management?

People undertake risk management activities to identify, assess, manage, and control all kinds of events or situations. These can range from single projects or narrowly defined types of risk, e.g. market risk, to the threats and opportunities facing the organisation as a whole. The principles presented in this position statement can be used to guide the involvement of internal audit in all forms of risk management but we are particularly interested in enterprise-wide risk management because this is likely to improve an organisation's governance processes.

Enterprise-wide risk management (ERM) is a structured, consistent and continuous process across the whole organisation for identifying, assessing, deciding on responses to and reporting on opportunities and threats that affect the achievement of its objectives.

Responsibility for ERM

The board has overall responsibility for ensuring that risks are managed. In practice, the board will delegate the operation of the risk management framework to the management team, who will be responsible for completing the activities below. There may be a separate function that co-ordinates and project-manages these activities and brings to bear specialist skills and knowledge.

Everyone in the organisation plays a role in ensuring successful enterprise-wide risk management but the primary responsibility for identifying risks and managing them lies with management.

Benefits of ERM

ERM can make a major contribution towards helping an organisation manage the risks to achieving its objectives. The benefits include:

- Greater likelihood of achieving those objectives;
- Consolidated reporting of disparate risks at board level;
- Improved understanding of the key risks and their wider implications;
- Identification and sharing of cross business risks;
- Greater management focus on the issues that really matter;
- Fewer surprises or crises;
- More focus internally on doing the right things in the right way;
- Increased likelihood of change initiatives being achieved;
- Capability to take on greater risk for greater reward and
- More informed risk-taking and decision-making.

The activities included in ERM

- Articulating and communicating the objectives of the organisation;
- Determining the risk appetite of the organisation;
- Establishing an appropriate internal environment, including a risk management framework;
- Identifying potential threats to the achievement of the objectives;
- Assessing the risk i.e. the impact and likelihood of the threat occurring;
- Selecting and implementing responses to the risks;
- Undertaking control and other response activities;
- Communicating information on risks in a consistent manner at all levels in the organisation;
- Centrally monitoring and coordinating the risk management processes and the outcomes, and
- Providing assurance on the effectiveness with which risks are managed.

The Institute of Internal Auditors

The Institute of Internal Auditors
UK and Ireland

Position statement:
The Role of Internal Audit in Enterprise-wide Risk Management

Providing assurance on ERM

One of the key requirements of the board or its equivalent is to gain assurance that risk management processes are working effectively and that key risks are being managed to an acceptable level.

It is likely that assurance will come from different sources. Of these, assurance from management is fundamental. This should be complemented by the provision of objective assurance, for which internal audit is a key source. Other sources include external audit and independent specialist reviews. Internal audit will normally provide assurances on three areas:

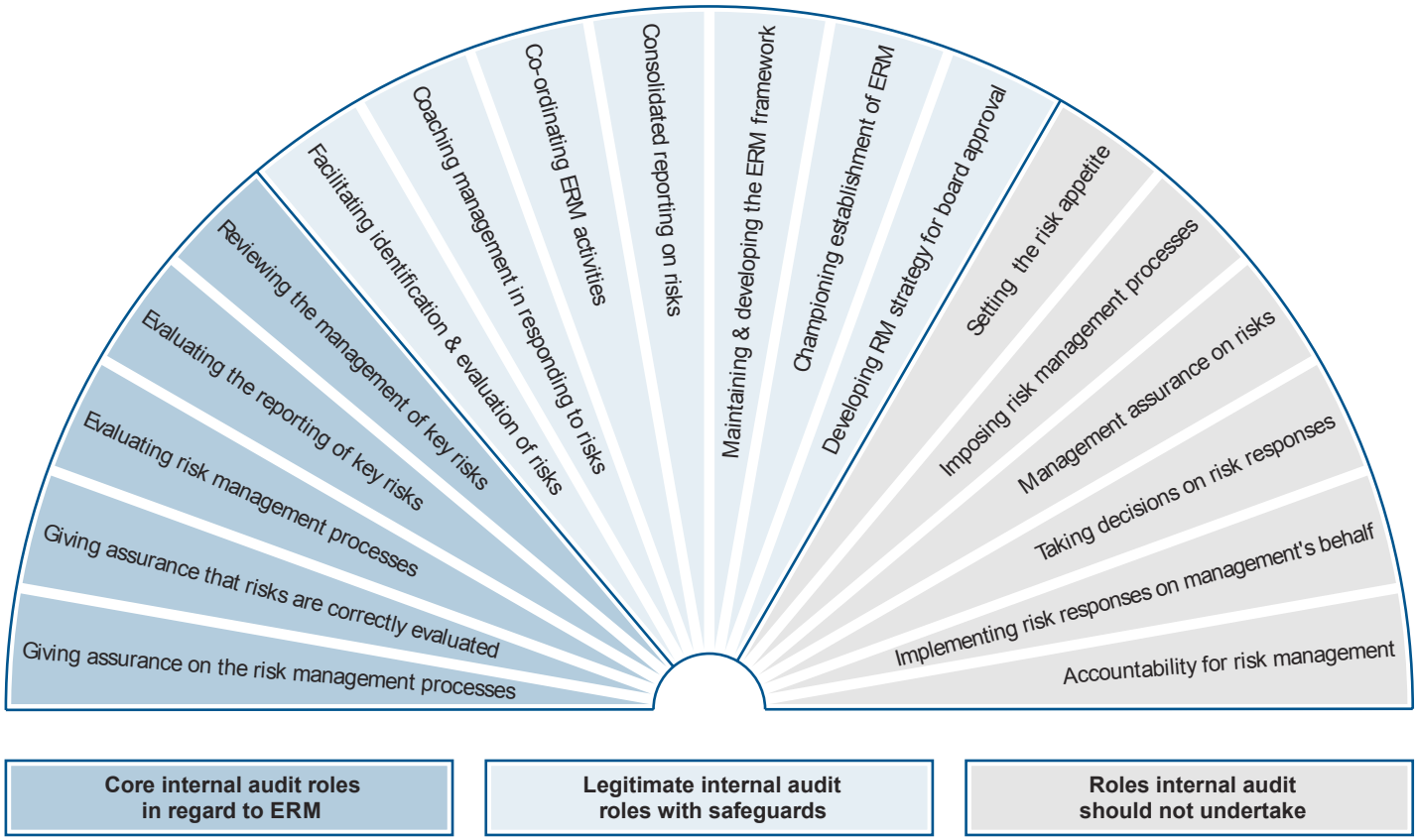
- Risk management processes, both their design and how well they are working;
- Management of those risks classified as 'key', including the effectiveness of the controls and other responses to them; and
- Reliable and appropriate assessment of risks and reporting of risk and control status.

The role of internal audit in ERM

Internal auditing is an independent, objective assurance and consulting activity. Its core role with regard to ERM is to provide objective assurance to the board on the effectiveness of risk management. Indeed, research has shown that board directors and internal auditors agree that the two most important ways that internal audit provides value to the organisation are in providing objective assurance that the major business risks are being managed appropriately and providing assurance that the risk management and internal control framework is operating effectively[1].

Figure 1 presents a range of ERM activities and indicates which roles an effective professional internal audit function should and, equally importantly, should not undertake. The key factors to take into account when determining internal audit's role are whether the activity raises any threats to the internal audit function's independence and objectivity and whether it is likely to improve the organisation's risk management, control and governance processes.

Figure 1 – Internal audit role in ERM



Position statement:
The Role of Internal Audit in Enterprise-wide Risk Management

The activities on the left of *Figure 1* are all assurance activities. They form part of the wider objective of giving assurance on risk management. An internal audit function complying with the *International Standards for the Professional Practice of Internal Auditing* can and should perform at least some of these activities.

Internal audit may provide consulting services that improve an organisation's governance, risk management, and control processes. The extent of internal audit's consulting in ERM will depend on the other resources, internal and external, available to the board and on the risk maturity[2] of the organisation and it is likely to vary over time. Internal audit's expertise in considering risks, in understanding the connections between risks and governance and in facilitation mean that it is well qualified to act as champion and even project manager for ERM, especially in the early stages of its introduction. As the organisation's risk maturity increases and risk management becomes more embedded in the operations of the business, internal audit's role in championing ERM may reduce. Similarly, if an organisation employs the services of a risk management specialist or function, internal audit is more likely to give value by concentrating on its assurance role, than by undertaking the more consulting activities. However, if internal audit has not yet adopted the risk-based approach represented by the assurance activities on the left of *Figure 1*, it is unlikely to be equipped to undertake the consulting activities in the centre.

Consulting roles

The centre of *Figure 1* shows the consulting roles that internal audit may undertake in relation to ERM. In general the further to the right of the dial that internal audit ventures, the greater are the safeguards that are required to ensure that its independence and objectivity are maintained. Some of the consulting roles that internal audit may undertake are:

- Making available to management tools and techniques used by internal audit to analyse risks and controls;
- Being a champion for introducing ERM into the organisation, leveraging its expertise in risk management and control and its overall knowledge of the organisation;
- Providing advice, facilitating workshops, coaching the organisation on risk and control and promoting the development of a common language, framework and understanding;
- Acting as the central point for coordinating, monitoring and reporting on risks; and
- Supporting managers as they work to identify the best way to mitigate a risk.

The key factor in deciding whether consulting services are compatible with the assurance role is to determine whether the internal auditor is assuming any management responsibility. In the case of ERM, internal audit can provide consulting services so long as it has no role in actually managing risks – that is management's responsibility – and so long as senior management actively endorses and supports ERM. We recommend that, whenever internal audit acts to help the management team to set up or to improve risk management processes, its plan of work should include a clear strategy and timeline for migrating the responsibility for these activities to members of the management team.

Safeguards

Internal audit may extend its involvement in ERM, as shown in *Figure 1*, provided certain conditions apply. The conditions are:

- It should be clear that management remains responsible for risk management.
- The nature of internal audit's responsibilities should be documented in the audit charter and approved by the Audit Committee[3].
- Internal audit should not manage any of the risks on behalf of management.
- Internal audit should provide advice, challenge and support to management's decision making, as opposed to taking risk management decisions themselves.
- Internal audit cannot also give objective assurance on any part of the ERM framework for which it is responsible. Such assurance should be provided by other suitably qualified parties[4].
- Any work beyond the assurance activities should be recognised as a consulting engagement and the implementation standards related to such engagements should be followed[5].

Skills and body of knowledge

Internal auditors and risk managers share some knowledge, skills and values. Both, for example, understand corporate governance requirements, have project management, analytical and facilitation skills and value having a healthy balance of risk rather than extreme risk-taking or avoidance behaviours. However, risk managers as such serve only the management of the organisation and do not have to provide independent and objective assurance to the audit committee. Nor should internal auditors who seek to extend their role in ERM underestimate the risk managers' specialist areas of knowledge (such as risk transfer and risk quantification and modelling techniques) which are outside the body of knowledge for most internal auditors. Any internal auditor who cannot demonstrate the appropriate skills and knowledge should not undertake work in the area of risk management. Furthermore, the head of internal audit should not provide consulting services in this area if adequate skills and knowledge are not available within the internal audit function and cannot be obtained from elsewhere[6].

[1]The Value Agenda, Institute of Internal Auditors – UK and Ireland and Deloitte & Touche 2003 [2]The IIA-UK and Ireland Position Statement on Risk Based Internal Auditing 2003
[3]Attribute Standard 1000.C1 [4]Attribute Standard 1130 [5]Perfomance Standards 2010,C1, 2110.C1 & C2, 2120.C1 & C2, 2130.C1, 2201.C1, 2210.C1, 2220.C1, 2240.C1, 2330.C1, 2410.C1, 2440.C1 & C2 and 2500.C1 [6]Attribute Standard 1210

Position statement:
The Role of Internal Audit in Enterprise-wide Risk Management

Conclusion

Risk management is a fundamental element of corporate governance. Management is responsible for establishing and operating the risk management framework on behalf of the board. Enterprise-wide risk management brings many benefits as a result of its structured, consistent and coordinated approach. Internal audit's core role in relation to ERM should be to provide assurance to management and to the board on the effectiveness of risk management. When internal audit extends its activities beyond this core role, it should apply certain safeguards, including treating the engagements as consulting services and, therefore, applying all relevant Standards. In this way, internal audit will protect its independence and the objectivity of its assurance services. Within these constraints, ERM can help raise the profile and increase the effectiveness of internal audit.

Glossary of terms

Assurance Services: An objective examination of evidence for the purpose of providing an independent assessment on risk management, control, or governance processes for the organisation. Examples may include financial, performance, compliance, system security, and due diligence engagements.

Board: A board is an organisation's governing body, such as a board of directors, supervisory board, head of an agency or legislative body, board of governors or trustees of a non profit organisation.

Champion: Someone who supports and defends a person or cause. Therefore, a champion of risk management will promote its benefits, educate an organisation's management and staff in the actions they need to take to implement it and will encourage them and support them in taking those actions.

Consulting Services: Advisory and related client service activities, the nature and scope of which are agreed with the client and which are intended to add value and improve an organisation's governance, risk management, and control processes without the internal auditor assuming management responsibility. Examples include counsel, advice, facilitation, and training.

Control: Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved.

Enterprise: Any organisation established to achieve a set of objectives.

Enterprise-wide risk management (ERM): A structured, consistent and continuous process across the whole organisation for identifying, assessing, deciding on responses to and reporting on opportunities and threats that affect the achievement of its objectives.

Facilitating: Working with a group (or individual) to make it easier for that group (or individual) to achieve the objectives that the group has agreed for the meeting or activity. This involves listening, challenging, observing, questioning and supporting the group and its members. It does not involve doing the work or taking decisions.

Risk: The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.

Risk Appetite: The level of risk that is acceptable to the board or management. This may be set in relation to the organisation as a whole, for different groups of risks or at an individual risk level.

Risk Management Framework: The totality of the structures, methodology, procedures and definitions that an organisation has chosen to use to implement its risk management processes.

Risk Management Processes: Processes to identify, assess, manage, and control potential events or situations, to provide reasonable assurance regarding the achievement of the organisation's objectives.

Risk Maturity: The extent to which a robust risk management approach has been adopted and applied, as planned, by management across the organisation to identify, assess, decide on responses to and report on opportunities and threats that affect the achievement of the organisation's objectives.

Risk Responses: The means by which an organisation elects to manage individual risks. The main categories are to tolerate the risk; to treat it by reducing its impact or likelihood; to transfer it to another organisation or to terminate the activity creating it. Internal controls are one way of treating a risk.

Position statement:
The Role of Internal Audit in Enterprise-wide Risk Management

Further reading

If you would like to find out more about the subject of risk management the following publications may be of interest to you:

Publication and Author	Publisher
Risk Management: Changing the Internal Auditor's Paradigm by Georges Selim and David McNamee	IIA Research Foundation
IIA Professional Briefing Note 13: Managing Risk	IIA-UK and Ireland
The Complete Guide to Business Risk Management by Kit Sadgrove	Gower
Operational Risk and Resilience: Understanding and minimising operational risk to secure shareholder value by PriceWaterhouseCoopers	Butterworth Heinemann
Risk Management Guide 2001	White Page
It's a Risky Business	CIPFA
The Risk Management Standard	IRM, AIRMIC and ALARM
ANZ Risk Management Standard	Standards Australia and Standards New Zealand
Enterprise Risk Management Framework	COSO
Risk Management in the Public Services	CIPFA & ALARM
Independence and Objectivity – Professional Issues Bulletin 2003	IIA - UK and Ireland
Embedding Risk Management into the Culture of your organisation – Professional Briefing Note 2003	IIA - UK and Ireland
Managing business risk – Adam Jolly	IOD, Ernst & Young and Kogan Page
The universe of risk – Pamela Shimell	Pearson Education and FT
Management of risk – OGC	TSO
Enterprise wide risk management – James Deloach	Pearson Education and FT
Risk – John Adams	Routledge
Risk management for company executives – John Smullen	Pearson Education and Financial Times Prentice Hall
Enterprise Risk Management: Trends & Emerging Practices – Miccolis, Hively, and Merkley	IIA Research Foundation
Enterprise Risk Management: Pulling it All Together – Walker, Shenkir and Barton	IIA Re search Foundation

You may also find the following websites of interest:

Website Address	Title or Organisation
www.theiia.org	The Institute of Internal Auditors
www.iia.org.uk	Institute of Internal Auditors – UK and Ireland
www.gee.co.uk	Gee Publishing
www.corpgov.net	Corporate Governance Site
www.coso.org	The Committee for Sponsoring Organizations (COSO)
www.theirm.org	The Institute of Risk Management (IRM)
www.airmic.com	The Association of Insurance and Risk Managers (AIRMIC)
www.alarm-uk.com	The National Forum for Risk Management in the Public Sector (ALARM)
www.whitepage.co.uk	White Page web-site
www.standards.org.au	Standards Australia
www.standards.co.nz	Standards New Zealand

Position statement:
The Role of Internal Audit in Enterprise-wide Risk Management

About the Institute

Established in 1941, The Institute of Internal Auditors (IIA) is an international professional association with global headquarters in Altamonte Springs, Florida, USA. The IIA has more than 95,000 members in internal auditing, risk management, governance, internal control, IT audit, education, and security. With representation from more than 160 countries, The Institute is the recognized authority, principal educator, and acknowledged leader in certification, research and technological guidance for the profession worldwide.

Copyright

About position statements

Position statements are part of a range of technical and professional guidance prepared by the Institute for its members. They are designed to clarify The IIA's official policy position on important and potentially complex matters confronting internal auditors.

For details of other guidance material provided by The Institute please visit our website, www.theiia.org

Disclaimer

This technical guidance material is not intended to provide definitive answers to specific individual circumstances and as such is only intended to be used as a guide. The Institute recommends that you always seek independent expert advice relating directly to any specific situation. The Institute accepts no responsibility for anyone placing sole reliance on this technical guidance.

The Institute of Internal Auditors
UK and Ireland

www.iia.org.uk

Institute of Internal Auditors – UK and Ireland Ltd
13 Abbeville Mews, 88 Clapham Park Road, London SW4 7BX UK
Telephone +44 (0) 20 7498 0101
Fax +44 (0) 20 7978 2492
Email technical@iia.org.uk
Registered in England and Wales, no. 1 474735

The Institute of Internal Auditors

www.theiia.org

The Institute of Internal Auditors
247 Maitland Avenue, Altamonte Springs, Florida 32701, USA
Telephone +1-407-937-1100
Fax +1-407-937-1101
Email issues@theiia.org