The Institute of Internal Auditors

# IIA POSITION PAPER:

# THE ROLE OF INTERNAL AUDITING IN ENTERPRISE-WIDE RISK MANAGEMENT

## Introduction

The importance to strong corporate governance of managing risk has been increasingly acknowledged. Organizations 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 organizations recognize their advantages over less coordinated approaches to risk management. Internal auditing, in both its assurance and its consulting roles, contributes to the management of risk in a variety of ways.

## 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 organization as a whole. The principles presented in this paper can be used to guide the involvement of internal auditing in all forms of risk management but we are particularly interested in enterprise-wide risk management because this is likely to improve an organization's governance processes.

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

## Responsibility for ERM

*T*he 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 organization 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 organization 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;
- *F*ewer 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 organization;
- Determining the risk appetite of the organization;
- 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 organization;
- Centrally monitoring and coordinating the risk management processes and the outcomes, and
- Providing assurance on the effectiveness with which risks are managed.

**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 the internal audit activity is a key source. Other sources include external auditors and independent specialist reviews. Internal auditors 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.

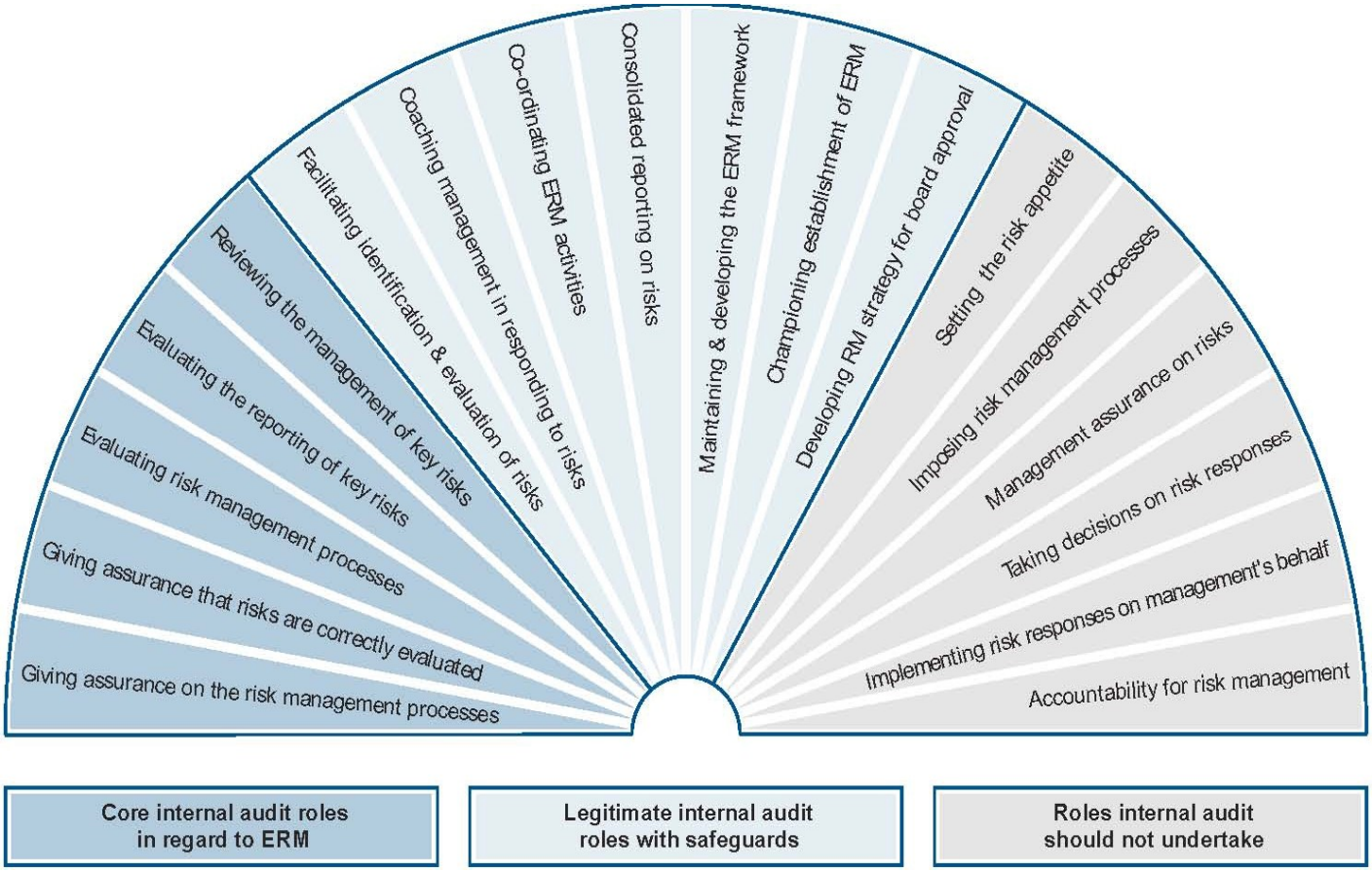
**The role of internal auditing in ERM**

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 auditing provides value to the organization 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].

[1] The Value Agenda, Institute of Internal Auditors – UK and Ireland and Deloitte & Touche 2003

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

**Figure 1 – Internal auditing's role in ERM**




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 activity complying with the *International Standards for the Professional Practice of Internal Auditing* can and should perform at least some of these activities.

Internal auditing may provide consulting services that improve an organization's governance, risk management, and control processes. The extent of internal auditor'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 organization and it is likely to vary over time. Internal auditor's expertise in considering risks, in understanding the connections between risks and governance and in facilitation mean that the internal audit activity is well qualified to act as champion and even project manager for ERM, especially in the early stages of its introduction. As the organization's risk maturity increases and risk management becomes more embedded in the operations of the business, internal auditing's role in championing ERM may reduce. Similarly, if an organization employs the services of a risk management specialist or function, internal auditing is more likely to give value by concentrating on its assurance role, than by undertaking the more consulting activities. However, if internal auditing 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 center.

**Consulting roles**

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

- Making available to management tools and techniques used by internal auditing to analyze risks and controls;
- Being a champion for introducing ERM into the organization, leveraging its expertise in risk management and control and its overall knowledge of the organization;
- Providing advice, facilitating workshops, coaching the organization 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 auditing 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 the internal audit activity 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 services to members of the management team.

[2] The IIA-UK and Ireland Position Statement on Risk Based Internal Auditing 2003

## Safeguards

Internal auditing 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 auditor's responsibilities should be documented in the internal audit charter and approved by the audit committee.
- Internal auditing should not manage any of the risks on behalf of management.
- Internal auditing should provide advice, challenge and support to management's decision making, as opposed to taking risk management decisions themselves.
- Internal auditing 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.
- Any work beyond the assurance activities should be recognized as a consulting engagement and the implementation standards related to such engagements should be followed.

## 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 behaviors. However, risk managers as such serve only the management of the organization 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 modeling 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 activity and cannot be obtained from elsewhere.

## 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 auditor'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 auditing 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 auditing 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 auditing.

**Definition of terms**

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

***Board:*** A board is an organization'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 organization, or any other designated body of the organization, including the audit committee to whom the chief audit executive may functionally report.

***Champion:*** Someone who supports and defends a person or cause. Therefore, a champion of risk management will promote its benefits, educate an organization'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, are intended to add value and improve an organization'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 organization established to achieve a set of objectives.

***Enterprise-wide risk management (ERM):*** A structured, consistent and continuous process across the whole organization 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 an organization is willing to accept.

***Risk Management Framework:*** The totality of the structures, methodology, procedures and definitions that an organization 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 organization's objectives.

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

***Risk Responses:*** The means by which an organization 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 organization or to terminate the activity creating it. Internal controls are one way of treating a risk.

***