RSM Bird Cameron
Chartered Accountants

Interfacing risk management and internal audit - conflicting or complementary?

By Angus Dickinson, Principal, Head of Risk Management Services, Sydney, RSM Bird Cameron

- Tone at the top messages must enable a clear understanding of the level of risk that is acceptable
- Legitimate areas do exist where internal audit and risk management functions can overlap, but care needs to be taken to manage these situations
- Imperative that internal audit maintains independence from the management function in assessing the adequacy of risk management

The roles of risk management and internal audit, as part of the overall governance structures of organisations, have been the subject of ongoing debate since the first modern reviews of corporate governance were initiated some 20 years ago.

Multiple national and international reviews have since published findings that have addressed overall governance principles, but have been unclear in their assessment of whether risk management and internal audit should be integrated, completely independent, or operate within a tailored structure that suits the particular requirements of the organisation, and enables coordinated interaction.

The fact that the debate continues today, with respected advocates of both risk management and internal audit holding firm but conflicting views is a testament that it is a question that is not easily answered.

It is generally accepted within today's governance models that, among the key components are the risk management and internal audit functions. The respective roles are defined as:

- risk management – 'coordinated activities to direct and control an organization with regard to risk'[1]
- internal audit – 'internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes'.[2]

Complicating factors

Given these definitions, it is apparent that the responsibility for managing risk within an organisation rests with operational management, whereas internal audit is independent of operational management and performs assurance and consulting activities designed to independently assess the effectiveness of the processes implemented by operational management.

Sounds simple enough ... but is it?

The problems that tend to blur the issue are driven by such factors as:

- organisational structures that result from differing governance models,

that require modification from those that are envisaged by the generic frameworks;

- uncertainty regarding the respective roles and responsibilities of the risk management and internal audit functions. This is generally driven by flawed internal reporting structures that confuse the responsibilities of each function;
- either function lagging behind the other – for example, it is difficult for internal audit to comment constructively with regard to risk management practices if these are limited or immature;
- knowledge levels and understanding of operational management of the respective roles and responsibilities of risk management and internal audit; and
- use of differing risk management and internal audit frameworks, and determination of who owns these frameworks.

This article seeks to consider the respective roles and responsibilities of risk management and internal audit functions.

Embedding risk management

Risk management is, at the highest level of an organisation, the establishment of protocols designed to enable defined strategies to be addressed and achieved through a process that evaluates the exposures an organisation faces, and implements measures to enable risks and opportunities to be managed to a level considered appropriate to the risk appetite.

The highest level of risk that an organisation faces is, quite simply, that it will fail to achieve its objectives. This may be through the failure to recognise opportunities and to convert these into achievements, the occurrence of adverse events, or conducting activities in an inefficient and ineffective manner that impedes the achievement of its objectives.

If the level of risk that an organisation is prepared to accept is not defined, there is potential for decisions being taken without an appreciation that its strategies will not be achieved. As the most significant risks that any organisation faces result from the decisions of its board or governing body, it is critical that the correct messages are communicated such that the level of risk that the organisation is prepared to accept is embedded within the psyche and is understood at all levels. The message that is sent – the 'tone at the top' – must provide both an understanding of the level of risk that can be accepted, and that the responsibility for risk management is then cascaded throughout the various levels of the organisation. Risk management is not just a concept; it needs to be understood, appreciated, and practised by everyone within the organisation.

Cascading the responsibility for risk management down through an organisation may mean that risks are identified within divisions or departments that are important to that division, but may have little impact upon the achievement of the organisation-wide objectives. In order to ensure that this occurs, there have to be clear linkages of identified risks to organisation-wide strategies, and a process that enables risks identified within a division or department that do affect the strategies and goals to be effectively escalated to the board on a timely basis.

Roles of management and internal audit in risk management

There are various models of governance, but the generally accepted models are two of the main components of any governance structure the effectiveness of management's risk management practices and the internal audit's monitoring of how effective these practices are. Guidance is provided within standards on how responsibilities should be shared within these roles.

The International Risk Management Standard, ISO 31000 (AS/NZS 31000:2009), is quite clear in defining the responsibilities of management. Management should:

- define and endorse the risk management policy;
- ensure that the organization's culture and risk management policy are aligned;
- determine risk management performance indicators that align with performance indicators of the organization;
- align risk management objectives with the objectives and strategies of the organization;

The highest level of risk that an organisation faces is, quite simply, that it will fail to achieve its objectives. Risk management is not just a concept; it needs to be understood, appreciated, and practised by everyone within the organisation.

- ensure legal and regulatory compliance;
- assign accountabilities and responsibilities at appropriate levels within the organization;
- ensure that the necessary resources are allocated to risk management;
- communicate the benefits of risk management to all stakeholders; and
- ensure that the framework for managing risk continues to remain appropriate.[3]

However, ISO 31000 also goes on to define the organisational responsibilities (as opposed to the responsibilities of management). This encompasses all personnel within the organisation, as well as other stakeholders who have an interest and obligation in ensuring that risk management practices are effective:

Organizations should:

- measure risk management performance against indicators, which are periodically reviewed for appropriateness;
- periodically measure progress against, and deviation from, the risk management plan;
- periodically review whether the risk management framework, policy and plan are still appropriate, given the organizations' external and internal context;
- report on risk, progress with the risk management plan and how well the risk management policy is being followed; and
- *review the effectiveness of the risk management framework.*[4]

While the obligation to create and maintain the risk management framework rests with management, there is also an obligation for the organisation to test the effectiveness of the risk management framework. How this is to be done is not stated within ISO 31000, but the distinction is that it is the management's responsibility to manage risk, and an organisation's responsibility to monitor risk is significant. Monitoring can be achieved either through implementation of a review structure established by management, through independent review (for example, by internal audit or other parties), or a combination of both.

Looking at the responsibilities of internal audit, *The International Standards for the Professional Practice of Internal Audit* (issued by the Institute of Internal Auditors (IIA)) states that 'the internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes'.

Standard 2120 goes on to explain the internal audit's role in greater detail, including:

2120.A1 – The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the:

- reliability and integrity of financial and operational information;
- effectiveness and efficiency of operations;
- safeguarding of assets; and
- compliance with laws, regulations and contracts.

2120.C3 – When assisting management in establishing or improving risk management processes, internal auditors must refrain from assuming any management responsibility by actually managing risks.[5]

Although ISO 31000 and the Internal Audit Standards have been issued by separate organisations, the concepts put forward regarding risk monitoring are complementary, provided conditions that enable independence when internal audit are applied.

The issue that exists as far as internal audit is concerned is how far do they get involved with risk management functions given their responsibility to evaluate the effectiveness of risk management and risk exposures, which requires independence from the functions they are evaluating, and their role of consulting to the organisation where their expertise can bring tangible benefits.

The IIA issued a Practice Advisory in January 2009 (which has been updated from earlier advisories) that defines how the role of internal audit should fit into the broader risk management structure, and, at the same time, achieve independence and enable internal audit to provide input in its consultative capacity. Figure 1 describes how the IIA envisages internal audit achieving its mandate, and those areas of risk management where internal audit should not get involved.

I find this diagram particularly useful as it provides a succinct summary of what can and cannot be conducted by internal audit. The central part of the diagram is the area where care needs to be taken, and where uncertainty arises about how closelyaligned and involved the functions of risk management and internal audit are.

Who owns the frameworks?

Risk management is a concept designed for use by an organisation to manage and control risk. As such, ownership of the framework must rest with those tasked within the organisation to manage risk and monitor the effectiveness of controls.

Internal audit's role is equally clear; it should assess the adequacy of the framework, the risk management processes, and the control environment with a view to identifying where gaps exist and reporting these to responsible management so that they can make appropriate decisions about how the identified matter should be addressed.

It is quite likely that there will be differences of opinion between internal audit and those tasked with risk management responsibilities. Internal audit has the responsibility to report matters where they believe that the response has been inadequate to the audit committee, and it is that body that should assess whether the organisational response has been adequate.

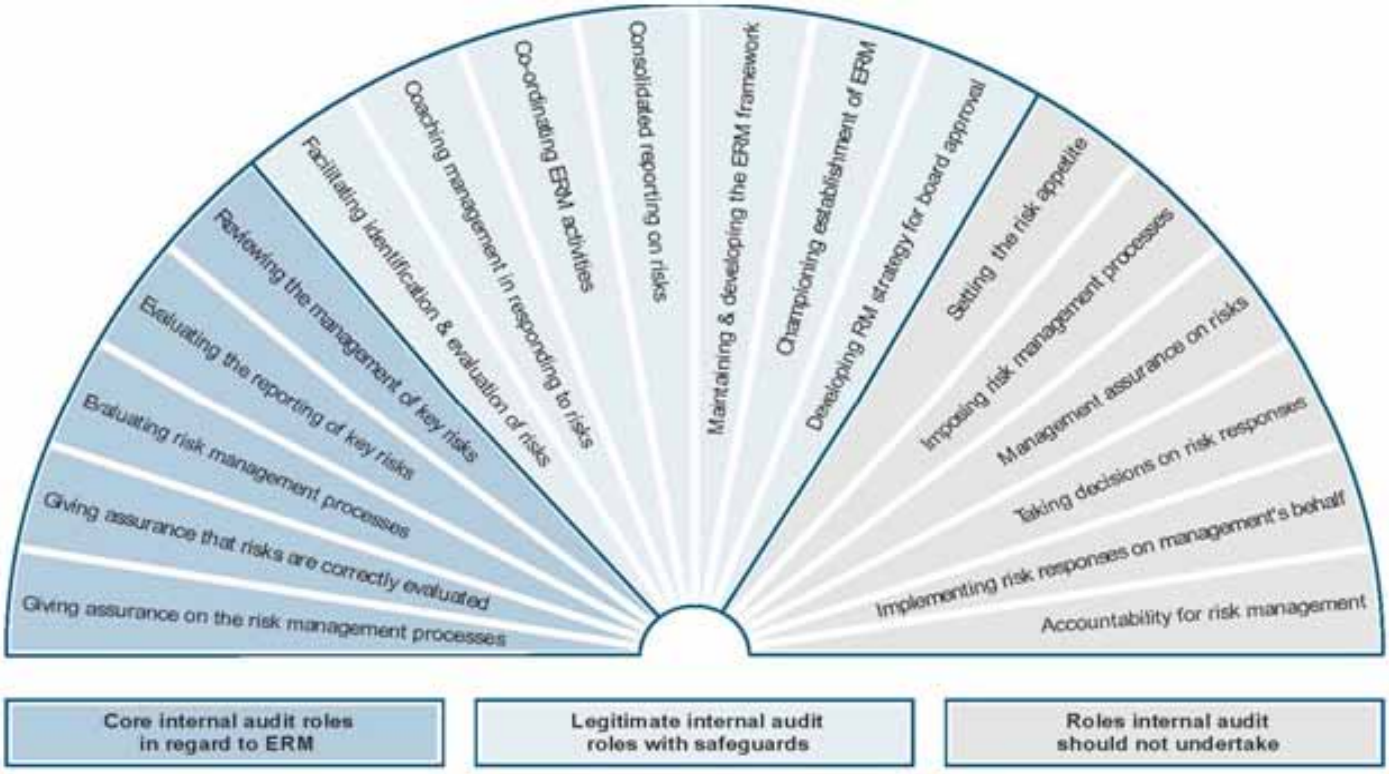
Organisational structures – the impact upon roles

When assessing the roles of risk management and internal audit in any organisation, there is a need to consider the differing reporting structures that exist within organisations. These structures often have a significant impact on the effective functioning of governance principles and dictate the respective roles of risk management and internal audit.

Broadly, the structures that are encountered within Australia fall into the following categories:

- larger corporate – including those that are subject to the ASX Corporate Governance Council Principals and Recommendations, that report to boards that are comprised of both executive and non-executive directors;
- SMEs – including private and family companies that report to boards comprised of persons who have a vested interest in the operations of the company, and lack the independence of a non-executive director;
- not-for-profit organisations – whose boards generally comprise of volunteers;
- government agencies – which operate with an executive management team reporting to a Director-General, who in turn reports to a responsible Minister;
- statutory authorities – which are subject to specific regulatory requirements, and invariably report through an appointed executive and board comprising of interested parties, through to a responsible Minister; and
- local government – where the general manager is responsible for all activities within the Council and has reporting obligations to both the council and to the responsible state government agency.

The differing structures and responsibilities do create difficulties in how to position both the risk management and internal audit functions within some organisations. Confusion does arise regarding respective roles – risk management is a tool of management, internal audit is a tool of the organisation – and this does result in circumstances where management seeks to steer internal



Reproduced with permission from the Institute of Internal Auditors. Extract from position paper *The Role of Internal Audit in Enterprise-wide Risk Management* (issued January 2009)

audit's focus away from a particular area of risk. Hence, it is imperative that internal audit maintains independence from the management function in conducting its assessment of the adequacy of risk management – if management exercises significant influence over what internal audit is able to do, the potential exists for areas of inefficiency, fraudulent activity and the like to escape internal audit's scrutiny.

Regardless of structure, there must be mechanisms to enable internal audit to operate independently, and for reporting channels to be in place that enables direct communication to the audit committee.

Take, for example, a debate that is currently being conducted within local government circles regarding the responsibility of the general manager to manage the entire operations of a council, which is specified in legislation. This is viewed by some to mean that the general manager should manage all activities within the sphere of the council's operations, including dictating what activities are conducted by both risk management and internal audit. This approach, apart from contravening internal audit standards by compromising internal audit's independence, means that a general manager could direct internal audit away from areas of high risk. A far better view of this organisational structure would be for internal audit to take its direction from the audit committee within a broad framework that is agreed between the audit committee and general manager, while leaving internal audit with the flexibility to determine a work program independent of influence from the general manager. Risk management would be the function that the general manager would work with to ensure that the management of risk was being conducted effectively.

Differing responsibilities, complementary functions

There are a variety of opinions about how the relationship between risk management and internal audit should be structured. There are some organisations that:

- maintain risk management and internal audit as two distinct functions reporting into separate audit and risk committees;
- maintain risk management and internal audit as two distinct functions reporting into a combined audit and risk committee;
- integrate risk management and internal audit under the responsibility of a single person, although the two functions are separate, and then report into a combined audit and risk committee; and
- combine the functions of risk management and internal audit into a single department (this is rare, and creates conflicts with the internal audit standards), and report into a combined audit and risk committee.

There is no doubt that each of these structures (and others) can work effectively provided that the personnel involved are able to recognise that they perform separate functions that, while complementary, have differing purposes.

Where problems arise, for example, is where regulators, who are not necessarily across the concepts of what comprises risk management and internal audit, mandate specific structures, rather than recognising that a 'one size fits all' does not suit some circumstances. Flexibility is provided within some structures, for example where the ASX Corporate Governance Council provides for the establishment of an audit committee[6] but does not discuss the establishment of a separate risk committee or a combined audit and risk committee. However, there are circumstances where specific structures are mandated such as with some policies adopted within government that specify that combined audit and risk committees should be established. This latter structure means that risk management and internal audit are forced into a structure that may lead to combining them within the organisation.

The important thing is to look at what works best. I have seen organisations that insist upon separate and distinct risk management and internal audit functions, which work extremely well provided there is continuous dialogue. I have also seen effective structures where risk management and internal audit are brought together functionally to ensure that there is continuous communication and cross-fertilisation of ideas in supporting their respective roles.

However, there are circumstances where the functions of risk management and internal audit do not operate effectively, with management dictating to internal audit in order to divert attention away from high risk areas. This is a dangerous situation, and why I generally counsel that, regardless of structure, there must be mechanisms to enable internal audit to operate independently, and for reporting channels to be in place that enables direct communication to the audit committee.

Conclusions

If you are looking for an answer, I am sorry to disappoint you … there is no right or wrong answer. Nor is there a single position that should be taken with regard to how the relationship between risk management and internal audit should be structured.

I liken the circumstances that we are dealing with to a couple of fencers who are training partners. Their training is dictated by the rules of fencing; each of them needs the other in order to develop their own skills, and they are continually testing each other to deal with opponents that they will face when they get into real competition.

Regardless of whether risk management and internal audit operate as distinct and separate units, or are closely aligned, it is imperative that they leverage off each other, continually developing knowledge and awareness of the environments in which they operate. They must work within the same risk management framework and conduct dialogue to continually question each other's perspective of the nature and severity of the risk profile.

Do they operate together or independently? This is quite clear – internal audit must maintain a degree of independence to ensure that they are in a position to critically assess the effectiveness of risk management and the adequacy of the control environment.

Do they report through the same structure in an organisation? This is not so clear – it really depends upon what works best. Larger, more structured organisations, will likely find that a clear separation of the two functions is best. Smaller and less structured organisations may find that bringing functional reporting through the same reporting channels creates synergies that are otherwise difficult to achieve. In reality, it comes down to whether the individuals concerned understand their respective roles, and are willing to adopt a pragmatic approach in making the relationship work effectively.

Notes

[1] ISO 31000:2009 Risk Management – Principles and Guidelines

[2] Institute of Internal Auditors: Definition of Internal Auditing

[3] Section 4.2 – Mandate

[4] Section 4.5 – Monitoring and Review of the Framework

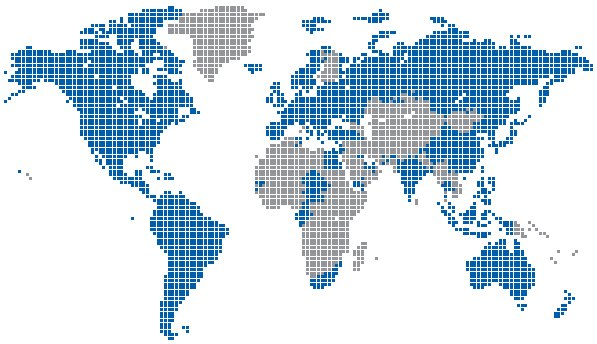
[5] IIA Standard 2120 – Risk Management, www.theiia.org

[6] ASX Corporate Governance Council, 2007, *Corporate Governance Principles and Recommendations*, Principle 4: Safeguard integrity in financial reporting

Angus Dickinson

Contact

RSM Bird Cameron
Level 12, 60 Castlereagh Street
Sydney NSW 2000
GPO Box 5138 Sydney NSW 2001
T +61 2 9233 8933
F +61 2 9233 8521
E angus.dickinson@rsmi.com.au



www.rsmi.com.au

This article was originally published in the Keeping good companies, Journal of Chartered Secretaries Australia Ltd, Vol.6, No.7, August 2010.