Broadleaf

Creating value from uncertainty

Broadleaf Capital International Pty Ltd

ABN 24 054 021 117

www.Broadleaf.com.au

Tutorial:
Relationship between internal audit and risk management

This short tutorial note addresses the relationship between the internal audit and risk management functions in organisations.

Version 1, 2014

Broadleaf

Contents

Tables

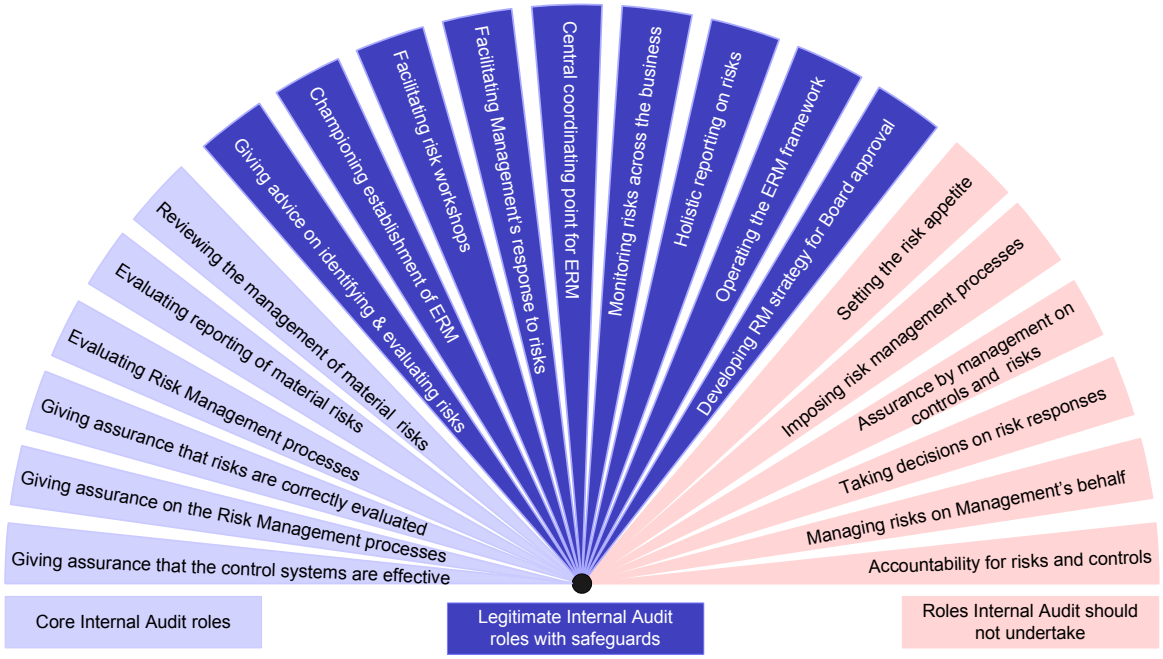
Figures

1 Tutorial

This note addresses the relationship between internal audit and risk management functions in organisations. For many years, audit functions have used information about risk, quite properly, as one of the core inputs to audit planning. For organisations without an effective enterprise risk management (ERM) function, or one in its early stages of development, this has meant that internal audit have been forced to undertake their own risk assessments; and in many circumstances internal audit have done their own assessments anyway as a check on risk management or to assert their independence. In addition, internal audit also have to audit risk management frameworks, to provide assurance to Boards and senior management about their adequacy and effectiveness. This is a requirement of the IIA Professional Practices Standards. It is also one way that Boards can satisfy the requirements of Principle 7.2 of the ASX Corporate Governance requirements.

Figure 1 below, reproduced from the Standards Australia and Institute of Internal Auditors handbook HB 158-2010, Delivering assurance based on ISO 31000:2009 Risk Management, illustrates a current view of the roles of internal audit and risk management. The dark-blue section in the middle of the fan is often the area of contention. Many internal auditors, and the firms who provide internal audit services on an out-sourced basis, would like to preserve the 'consulting' activities within their own domains.

Figure 1: Internal audit and risk management roles



Note: This diagram is taken from HB 158-2010 Delivering assurance based on ISO 31000:2009 Risk Management, and is itself based on a diagram in a position statement released by the Institute of Internal Auditors – UK and Ireland in September 2004 on The Role of Internal Audit in Enterprise-wide Risk Management.

Broadleaf's view is that the tasks in the dark-blue section of the fan should be separated from internal audit. Within most organisations there is a clear conflict of interest between internal audit and risk management in these areas. Some of the specific roles and activities that may lead to conflicts of interest are noted in Table 1.

Table 1: Areas of overlapping interest

Risk management	Internal audit
Develop the risk management framework	Audit the adequacy and effectiveness of the risk management framework
Implement the risk management framework	Audit implementation of the risk management framework
Advise management on integration of risk management into business operations and their roles in making it work	Audit management's commitment to risk management and the take up of their roles

Risk management	Internal audit
Advise on the allocation of accountability for risks, controls and tasks	Audit whether accountable managers fulfil those roles and are capable
Advise management and the Board on the interpretation of risk management information	Provide independent assurance of the risk management information submitted to the Board
Provide appropriate risk management status and performance information to the Board Audit Risk and Compliance Committee	Provide an independent view on the credibility and reliability of the risk management information submitted to the Board Audit Risk and Compliance Committee
Act as an advisor and mentor to management on risk management matters	Act as an independent reviewer to provide assurance on management's capability and performance in risk management

Having the internal audit and risk management functions report to one manager who then, presumably, presents both sets of reports and represents both functions to the Board or a Board Audit and Risk Committee is very difficult. While internal audit and risk management have to work together, we believe it is essential that they report to separate senior managers, for clear governance purposes and to ensure that neither role in compromised. Those Chief Risk Officers who must balance internal audit, risk management and compliance portfolios often struggle with this in practice.

Apart from governance matters of the kind discussed above, there are clear management and cultural reasons for separating internal audit and risk management. Risk management is a line management function – line managers are the people ultimately responsible for delivering business outcomes, and they are responsible for managing the risks in their areas of the organisation. Having risk management separated from the line and located in a central, compliance-related area sends mixed messages to the organisation. In our view it is far better to ensure a distinct separation of internal audit and risk management, with the central risk management team having custodianship of the overall risk management framework, process and data base, but line managers having clear responsibility for risk management. The risk management function can then act as a trainer and mentor to management, to support them in their role.

While separation is important, it is vital that the risk management process generates appropriate information for internal audit to allow the development

of assurance plans and timetables, including the Internal Audit Plan. Such information should include registers of the organisation's risks, the associated controls, management's assessment of the effectiveness of those controls, the consequences and likelihoods of each risk arising with the controls in their current state of effectiveness, and the potential exposure the organisation might face from each risk were the controls to fail completely.

Internal audit are also interested in risk treatment plans that represent management's commitment to respond to the current level of risk. They should review the integrity of the methodology that generated the actions in those plans and track progress in completing the actions. Internal audit are also concerned with the quality and effectiveness of line management review of controls and risks through the application of methods such as control self assessment.

2 Contact

If you would like further information about this topic please contact us. We will endeavour to reply promptly.

Dr Dale F Cooper
Cooper@Broadleaf.com.au

Pauline Bosnich
Bosnich@Broadleaf.com.au

Dr Stephen Grey
Grey@Broadleaf.com.au

Grant Purdy
Purdy@Broadleaf.com.au

Geoff Raymond
Raymond@Broadleaf.com.au

Phil Walker
Walker@Broadleaf.com.au

Mike Wood
Wood@Broadleaf.co.nz

For further information visit www.Broadleaf.com.au