The Institute of Internal Auditors Australia

Dear Q&A

Can internal audit and risk management be together under the same manager?

Answer

Organisations have what is called 'line 1' activities which are where the operational work gets done.

Many organisations also set up specialist advisory and monitoring functions over risk management, compliance, financial management and other activities. These specialist advisory functions are not responsible for making risk / compliance / finance/ human resources decisions but are there to monitor that these decisions are taken properly in accordance with rules, to provide advice in relation to these decisions, and to report on the results of this decision-making.

These specialist advisory and monitoring functions are the responsibility of 'line 2' managers. They advise, monitor and report but do not make decisions.

The reference to 'lines' in this context indicates the information gets to top management by different paths and therefore provides more than one perspective.

'Line 2' risk management is an ally of internal audit. Both functions are interested in the risk profile of the organisation and in improving management of risk. Internal Audit Standard 2120 'Risk Management' says "The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes".

However, the 'line 2' risk management specialist unit headed by the chief risk officer reports to executive management whereas internal audit is 'line 3' and reports to the board through the audit committee. Internal audit is designated 'line 3' because it provides information to the board in a manner that is independent of line management.

The IIA Global 'Three Lines Model' (2020) may help in understanding this distinction between the lines. The lines are conceptually distinct, but practicalities may mean one of the lines is missing or that internal audit ('line 3'), in the absence of a separate risk management function ('line 2'), takes over much of the risk management advisory role.

In many organisations risk management advisory and internal audit are combined. The same individual is both chief risk officer and chief audit executive (head of internal audit).

This requires some skill on the part of the holder of this position as for some of their function they report to executive management and for some they report to the board (audit committee).

Having both those roles vested in one person is sometimes necessary in small organisations where there are limited budgets and insufficient resources to separate them. In financial services, and in other organisations where there is a large and active risk management function, this is rarely done.

The ideal situation is that the chief risk officer and chief audit executive are different individuals, and the Internal Audit Standards warn about conflicts that might arise – Internal Audit Standard 1112 'Chief Audit Executive Roles Beyond Internal Auditing' – "Where the chief audit executive has or is expected to have roles and / or responsibilities that fall outside of internal auditing, safeguards must be in place to limit impairments to independence or objectivity".

This conflict can be managed by:

- Being clear about what are management 'line 1' and what are risk management 'line 2' roles. Risk management provides advice – it does not make decisions.
- Being clear about what are risk management 'line 2' and what are internal audit 'line 3' roles – refer IIA Global Position Paper 'The Role of Internal Auditing in Enterprise-wide Risk Management (ERM)' (2009)
- Provide safeguards such as clarity of reporting lines and independent review of risk management. While internal audit may undertake the monitoring and advisory roles of risk management, they cannot then review the risk management function, and this would need to be performed independently.

Need an answer? Send your questions through to IAassist@iia.org.au

The position paper on ERM has a useful diagram that shows what can or cannot be done by an internal auditor working in risk management. In a document by Standards Australia HB158-2010 'Delivering Assurance' this diagram was enhanced to show the legitimate role of the risk management advisor.

We would take the view that combining internal audit with risk management is less than ideal but is better than not having a risk management advisory function. Undesirable as combining chief risk officer and chief audit executive roles might be in theory, it is much better to combine them than to have the chief risk officer report to the chief audit executive or to have the chief audit executive report to the chief risk officer. A combined position is also better than having each report separately to a third person as such an arrangement lowers the access that both the chief risk officer and chief audit executive have to the board (audit committee) and senior members of the organisation.

It should be made clear that:

- Even a dedicated chief risk officer with a risk management team is only a facilitator. They should not be accountable for decisions made by line management, and it is those decisions that must be informed by risk assessment. When management need advice on risk, the chief risk officer's team is there to help provide it, but they cannot tell a responsible manager what their decision must be.
- The chief audit executive is obliged to provide advice to anything that is of relevance to the board's appetite for risk – no aspect of the chief audit executive's operations can be segregated from that process – refer Internal Audit Standard 2600 'Communicating the Acceptance of Risks' "When the chief audit executive concludes that management has accepted a level of risk that may be unacceptable to the organisation, the chief audit executive must discuss the matter with senior management. If the chief audit executive determines that the matter has not been resolved, the chief audit executive must communicate the matter to the board".

There is nothing in the Internal Audit Standards that precludes an internal auditor taking on this job, but it is necessary to make sure that there are safeguards and these are usually included in the internal audit charter.

The Institute of Internal Auditors Australia

Need an answer? Send your questions through to IAassist@iia.org.au