Connect › Support › Advance

The Institute of Internal Auditors Australia

White Paper

Internal Audit and Risk Management: Separate or Together?

February 2023

Level 5, 580 George Street, Sydney NSW 2000 | PO Box A2311, Sydney South NSW 1235
T +61 2 9267 9155 **F** +61 2 9264 9240 **E** enquiry@iia.org.au **www.iia.org.au**

Internal Audit and Risk Management: Separate or Together?

Contents

Background

Purpose

This White Paper has been written to analyse whether internal audit and risk management should be kept separate or located together.

Background

Internal audit and risk management are both assurance activities. They are both interested in risk, with internal audit using risk management theory and practice in its work. They are both focused on reducing risk to manageable levels. There is synergy between the two disciplines – interaction and cooperation producing a combined effect greater than separately.

A recurring theme in recent times has been whether it is a logical move to co-locate internal audit and risk management or to keep them distinctly separate.

Discussion

Issue

Internal audit and risk management are separate disciplines, but both are essential assurance activities.

Internal audit is positioned outside the management structure, while risk management reports directly to the management structure.

Some organisations keep internal audit and risk management separate, while some organisations choose to co-locate them.

The question to be discussed is:

> *Should internal audit and risk management be kept separate or located together?*

History

Internal audit in its modern-day form evolved from the 1940s through a process of evolution:

- Checking – up to 1960s – Simple checking of transactions to ensure correctness that often involved checking 100% of transactions.
- Compliance – 1960s–1980s – Simple compliance audits of individual business activities and transactions with a cyclical approach to cover every organisation activity over a number of years.
- System-Based – 1980s–1990s – Introduced the concept of end-to-end audits of system controls but maintained a cyclical approach to cover every organisation activity over a number of years.
- Risk-Based – 1990s–2010s – Internal audit accepted that limited budgets meant it could not audit everything, and also that some lower risk activities might not warrant the cost of an audit.
- Partnership – 2010s – Internal audit and management actively work together for the common good and success of their organisation, with internal audit maintaining its independence.
- Value-Based – emerging – A methodology where internal auditors perform forward-looking internal

Internal Audit and Risk Management: Separate or Together?

audit services to offer insights and actively seek innovation to improve an organisation, seeking to do this from the audit client perspective. Value-based auditing is where the internal audit profession is heading – not many internal audit functions are there yet, but it is an emerging trend.

For further information on internal audit's evolution over time, refer the IIA-Australia Factsheet 'Internal Audit Evolution'.

Risk management has been around as long as mankind, but its genesis as a recognised discipline with formal theory and practice started in the 1990s and culminated in a risk management standard in Australia in 2004 (Australian Standard 4360) followed by an international standard modelled on the Australian standard in 2009 (ISO 31000).

What is Risk?

Risk arises whenever we are trying to achieve an objective in an environment of uncertainty. It is expressed in terms of the potential consequences (impact) of that uncertainty and the likelihood (probability) of experiencing those consequences. The uncertainty may be unknown future events but is very often a shortage of information about the environment in which we are working.

The definition of 'risk' adopted in Australia in Australian Standard (AS) ISO 31000:2018' Risk management – Guidelines' reflects this:

> *'Effect of uncertainty on objectives.'*

What is Risk Management?

The Institute of Internal Auditors (IIA) has defined 'risk management' as:

> '*A process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of organisation objectives.'*

Risks are managed by those accountable for the delivery of the products and services of an organisation. A risk management function does not itself manage risks but manages an organisation's risk management framework, provides advice to operational management and coordinates reporting of risk status. For further information on the risk management function, refer the IIA-Australia Factsheet 'Risk Management'.

Key technical reference documents for risk management practice are:

- Australian Standard (AS) ISO 31000:2018 'Risk management – Guidelines'.
- COSO 'Enterprise Risk Management – Integrating with Strategy and Performance'.

Risk management is a management function and the 'risk management' function provides advice to management.

What is Internal Audit?

The definition of 'internal audit' is:

> '*An independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.'*

Internal audit does not manage risk but it does provide information in the form of assurances and advice to the board and management of an organisation. This information reduces the uncertainty faced by management and therefore contributes to management of risk. For further information on Internal Audit, refer the IIA-Australia Factsheet 'Internal Auditing'.

The key reference document for internal audit practice is:

- 'International Professional Practices Framework' (IPPF) issued by the Internal Audit Foundation.

Internal audit provides advice to those charged with governance.

Should Internal Audit and Risk Management be Separate or Together?

Both risk management and internal audit contribute to the management of risk within an organisation, although neither of these functions directly manage organisational risk.

Organisations have what is called Line 1 activities which

Internal Audit and Risk Management: Separate or Together?

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 resource 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 function headed by the chief risk officer reports to executive management whereas internal audit is Line 3 and reports to the board of directors / governing authority through the audit committee. Internal audit is designated Line 3 because it provides information to the board of directors / governing authority in a manner independent of line management.

The IIA Global 'Three Lines Model' (2020) can help understanding of this distinction between the lines. ISO 37000:2021 'Organisational governance – Guidelines' takes a similar approach recommending the governing authority should obtain assurance by obtaining:

- Direct verifications.
- Direct reports from and private sessions with risk management and compliance management as independent control functions.
- Direct reports from and private sessions with internal audit as an independent provider of assurance - including covering the effectiveness of the risk management and compliance management processes.

The Lines are conceptually distinct, but practicalities may mean one of the Lines is missing or that Line 3 internal audit, in the absence of a separate Line 2 risk management function, takes over much of the risk management advisory role.

In some organisations risk management advisory and internal audit are combined – the same individual is both chief risk officer and chief audit executive. This requires some skill on the part of the holder of these dual responsibilities 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 have two separate functions. In financial services and other organisations where there is a large and active risk management function, this is rarely done. Very large and complex organisations may even have multiple specialist risk management advisory functions.

The ideal situation is that the chief risk officer and chief audit executive are different individuals. Where both functions are co-located, conflict of interest needs to be managed.

This conflict can be managed by:

- Being clear about what are management Line 1 roles 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.

Internal Audit and Risk Management: Separate or Together?

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 the joint IIA-Australia / Standards Australia & Standards New Zealand publication HB158–2010 'Delivering Assurance Based on AS/NZS ISO 31000' (Finger, et al., 2010) this diagram was enhanced to show the legitimate role of the risk management advisor.

There is a 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 of anything 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 the risk advisory role, but it is necessary to make sure there are safeguards and these are usually included in the internal audit charter.

It should be noted that some jurisdictions ban 'dual-hatting' and mandate separation between risk management and internal audit such as required by the Australian Prudential Regulation Authority (APRA) for the financial services and insurance sector – refer Prudential Standard 220 'Risk Management'.

Research

In 2012 Dr Steven Halliday conducted research into the structure of risk management in the Australian S&P/ASX 200.

The study found at the time that 30% of S&P/ASX 200 Australian companies had:

- Integrated their internal audit and risk management teams at the functional level.
- A further 30% of companies indicated they had both internal audit and risk management reporting to a common executive officer, a partially integrated model.
- 30% of the population had strict separation between internal audit and risk management and the final 10% no risk management function.

Recent analysis by the IIA-Australia built on this research suggests advantages and disadvantages as shown on the following page.

Internal Audit and Risk Management: Separate or Together?

	Separate	Together
Leadership	› Clear leadership boundaries leading to clear independence.	› The concept of chief risk officer and chief audit executive being the same person provides clear leadership boundaries but detracts from internal audit independence.
Independence	› Clear independence and separation of Line 2 risk management and Line 3 internal audit. › Separate administrative reporting clearly demonstrates internal audit independence from management.	› Independence may become blurred and difficult to achieve or demonstrate to in-house business unit clients. › Two different administrative reports can be difficult – risk management reporting to management and internal audit reporting ideally to chief executive officer.
Synergy	› Synergy between the two activities can take more effort.	› Many people see internal audit as a sub-set of risk management with direct synergy between the two activities.
Professional Objectives	› Professional objectives clear.	› Professional objectives may become blurred.
Business Intelligence and Information Sharing	› It can be more difficult to share information. › Can make it more difficult for internal audit work to inform and update risk registers.	› Information can be more easily achieved. › Can make it easier for internal audit work to inform and update risk registers.
Efficiency and Effectiveness	› Larger organisations can ensure internal audit independence is not diluted (actual or perceived) by keeping the two activities separate.	› Resourcing of risk management and internal audit can be better achieved in smaller organisations if the two activities are co-located.
Maturity	› Less mature risk management and internal audit activities better suited to operating separately.	› Likely to be work better with mature risk management and internal audit activities.

Internal Audit and Risk Management: Separate or Together?

The Concept of Safeguards

The strength of internal audit comes from it being independent of management.

Where the chief audit executive may be responsible for a non-audit activity, for example risk management, safeguards need to be included in the internal audit charter so the chief audit executive cannot 'mark their own homework'. As well as being good governance practice, this is also a requirement of 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".*

Suggested safeguard wording for inclusion in the internal audit charter could be:

> *Where the chief audit executive may be responsible for a non-audit activity, there are independence safeguards in place:*
>
> - *When responsible for non-audit activities, the chief audit executive is not performing internal audit duties when managing or performing those activities; and*
> - *Internal audit review of non-audit activities under the control of the chief audit executive must be managed and performed independently of the chief audit executive and reported direct to the audit committee.*

The words shown are illustrative and can be replaced with other safeguard words – the point is there needs to be some form of safeguard included in the internal audit charter.

It does not mean that if the chief audit executive has responsibility for a non-audit business activity they cannot be involved in the audit process of that activity – it is important for a business activity owner to be involved in audits of topics for which they are responsible.

What it does mean is that where the chief audit executive is responsible for a non-audit business activity that is to be audited, they should not be involved in such things as (a) selecting the auditor to perform the audit (b) managing the auditor or service provider performing the audit (c) control over planning of performance of the audit (d) the internal audit report. This must be done at 'arm's length'.

They would, of course, be involved and contribute to such things as (a) input to the audit objectives and scope (b) providing information to the auditor (c) reviewing the draft internal audit report and providing feedback (d) providing periodic updates of audit action implementation progress after the audit.

They should not have overall control of the audit process which should be assigned to someone independent of the activity being reviewed. This could be the audit committee chair or an executive of at least the same job classification in a business area that receives few audits.

Conclusion

Summary

Internal audit and risk management are separate disciplines, but both are essential assurance activities. Internal audit is positioned outside the management structure, while risk management reports directly to the management structure.

Things to consider:

- If an organisation is sufficiently large with 'critical mass', there is no compelling argument to co-locate internal audit and risk management.
- A decision to separate internal audit and risk management should not be left to management alone – such a decision should only be made with a well-informed business case and concurrence of the board / audit committee for the decision.
- Where an organisation has a separate audit committee and risk management committee, the two activities should remain separate.
- A joint chief risk officer / chief audit executive arrangement requires formal independence safeguards.
- A joint chief risk officer / chief audit executive arrangement requires reporting arrangements of:
  - Internal audit – functionally to the audit committee through the chair and administratively

Internal Audit and Risk Management: Separate or Together?

to the chief executive officer.

- Risk management – functionally and administratively ideally to the chief executive officer.

- A joint chief risk officer / chief audit executive should never report to another executive.
- Chief audit executive performance assessment should be driven by the audit committee and not management. It makes absolutely no sense to establish internal audit as an independent Line 3 assurance activity – independent of Line 1 and Line 2 management – and then give management the role of assessing chief audit executive performance.

Conclusion

There are advantages and disadvantages to keeping risk management and internal audit separate and for a decision to co-locate them.

The decision is ultimately for an individual organisation to make.

Bibliography and References

ASX Corporate Governance Council. (2019). Corporate Governance Principles and Recommendations, 4th Edition. Sydney: ASX.
Retrieved from https://www.asx.com.au/documents/asx-compliance/cgc-principles-and-recommendations-fourth-edn.pdf

Australian Commission on Safety and Quality in Health Care. (2017). National Model Clinical Governance Framework.
Retrieved from Australian Commission on Safety and Quality in Health Care: https://www.safetyandquality.gov.au/sites/default/files/migrated/National-Model-Clinical-Governance-Framework.pdf

Australian Commission on Safety and Quality in Health Care. (2019, Mar). NSQHS Standards User Guide for Governing Bodies.
Retrieved from Australian Commission on Safety and Quality in Health Care: https://www.safetyandquality.gov.au/sites/default/files/2019-11/nsqhs_standards_user_guide_for_governing_bodies.pdf

Australian Commission on Safety and Quality in Health Care. (2021, May). National Safety and Quality Health Service Standards.
Retrieved from Australian Commission on Safety and Quality in Health Care: https://www.safetyandquality.gov.au/sites/default/files/2021-05/national_safety_and_quality_health_service_nsqhs_standards_second_edition_-_updated_may_2021.pdf

International Organization for Standardization. (2021). ISO 37000:2021 Governance of organizations - Guidance. Geneva: International Organization for Standardization.

The Institute of Internal Auditors - Australia. (2019). The 20 Critical Questions Series: What Directors should ask of Corporate Governance.
Retrieved from https://iia.org.au/sf_docs/default-source/technical-resources/20-critical-questions/20-questions-directors-should-ask-of-corporate-governance.pdf

The Institute of Internal Auditors - Australia. (2020). Factsheet: Corporate Governance.
Retrieved from https://iia.org.au/sf_docs/default-source/technical-resources/2018-fact-sheets/corporate-governance.pdf

The Institute of Internal Auditors - Australia. (2020). Factsheet: Corporate Governance Responsibility Matrix.
Retrieved from https://iia.org.au/technical-resources/knowledgeitem.aspx?ID=345

The Institute of Internal Auditors, Inc. (2020). The IIA's Three Lines Model: an update of the three lines of defense.
Retrieved from Institute of Internal Auditors - Global: https://www.theiia.org/en/content/position-papers/2020/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense/

Purpose of White Papers

A White Paper is a report authored and peer reviewed by experienced practitioners to provide guidance on a particular subject related to governance, risk management or control. It seeks to inform readers about an issue and present ideas and options on how it might be managed. It does not necessarily represent the position or philosophy of the Institute of Internal Auditors-Global and the Institute of Internal Auditors-Australia.

Internal Audit and Risk Management: Separate or Together?

Author Biographies

This White Paper written by:

Andrew Cox MBA, MEC, GradDipSc, GradCertPA, DipBusAdmin, DipPubAdmin, AssDipAcctg, CertSQM, PFIIA, CIA, CISA, CFE, CGAP, CSQA, MACS Snr, MRMIA

Andrew Cox is Manager of Technical Services at the IIA-Australia, responsible for technical matters including contributions to the body of knowledge around governance, risk management and internal audit.

He was previously a chief audit executive at significant organisations. He further developed the internal audit external quality assessment process in Australia and has performed more than 300 of these in corporate and public sector organisations in Australia, Bahrain, Brunei, Kuwait, Qatar, Saudi Arabia and the United Arab Emirates.

He has made presentations on internal auditing in forums in Australia and internationally and has taught internal auditing in Australia and other countries. He co-authored the IIA-Australia publication 'Internal Audit in Australia' and co-authored 'Audit Committees – A Guide to Good Practice, 3rd edition' issued by AICD / AUASB / IIA-Australia. He contributed to 'Sawyer's Internal Auditing, 7th Edition'.

He is an independent member of a number of audit committees.

Michael Parkinson BSc(Hons), GradDipComp, PFIIA, CIA, CISA, CRMA, CRISC

Michael is an internal auditor and risk management consultant in private practice. He has more than 30 years of experience in a range of government and non-government environments. He has been active in the development of risk management and internal auditing standards and guidance for more than 10 years. Michael has practiced in Australia and South East Asia and currently serves on a number of Audit and Risk Management Committees.

Michael has been the recipient of the IIA–Australia Bob McDonald Award and the IIA-Global Victor Z Brink Award for services to the profession of internal auditing.

This White Paper edited by:

Tracy Piscopo GradCertBus(PSM), GradCertIA, CertAL, PMIIA, PMIPAA, MAICD

Lee Sullivan BComm, PFIIA, GAICD, CA, EMBA, ANZIIF(Fellow), CIP

About the Institute of Internal Auditors-Australia

The Institute of Internal Auditors (IIA) is the global professional association for Internal Auditors, with global headquarters in the USA and affiliated Institutes and Chapters throughout the world including Australia.

As the chief advocate of the Internal Audit profession, the IIA serves as the profession's international standard-setter, sole provider of globally accepted internal auditing certifications, and principal researcher and educator.

The IIA sets the bar for Internal Audit integrity and professionalism around the world with its 'International Professional Practices Framework' (IPPF), a collection of guidance that includes the 'International Standards for the Professional Practice of Internal Auditing' and the 'Code of Ethics'.

The IIA-Australia ensures its members and the profession as a whole are well-represented with decision-makers and influencers, and is extensively represented on a number of global committees and prominent working groups in Australia and internationally.

The IIA was established in 1941 and now has more than 200,000 members from 190 countries with hundreds of local area Chapters. Generally, members work in internal auditing, risk management, governance, internal control, information technology audit, education, and security.

Internal Audit and Risk Management: Separate or Together?