The Institute of Internal Auditors Australia

CAE '60 Second' Survey

Internal Audit and Risk Management – Separate or Together?

February/March 2023

Introduction

Risks are managed by those accountable for the delivery of the products and services of an organisation. A risk management advisory/coordination 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. Similarly internal audit does not manage risk but provides information in the form of assurances and advice to those who manage risk (The Institute of Internal Auditors - Australia, 2022).

The risk management advisory/coordination function and internal audit both contribute to the management of risk in an organisation. They have much in common and should work together for the benefit of their organisation.

Large and complex organisations or those with highly technical risks to manage frequently establish separate risk committees at executive (and sometimes board) level.

Risk management is a management activity and, as a consequence, the risk management advisory/coordination function (advising management) is generally characterised as Line 2 rather than Line 3 (The Institute of Internal Auditors, Inc, 2020). Many organisations separate the two sets of activities but this is not always practical. While the IIA has taken the view that most functions ordinarily conducted by a risk management advisory/coordination function may be conducted by the internal audit function, provided appropriate safeguards are in place to maintain the internal auditor's independence and objectivity (The Institute of Internal Auditors, 2009), this is not ideal (Cox & Parkinson, 2023).

For the remainder of this paper we will use the term "risk management" to refer to the advice and coordination activity.

The Survey

The Institute of Internal Auditors – Australia surveyed Chief Audit Executives (CAEs) to explore the way in which these functions are established in Australian organisations. 73 responses were received across a wide section of the economy (Exhibit 1).

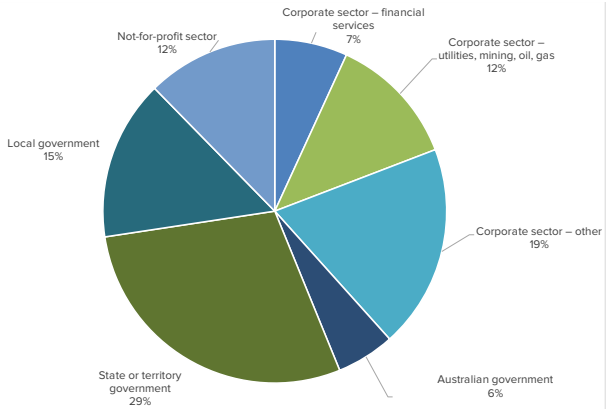

Exhibit 1 – Economic sector of respondents

Governance Arrangements

The normal approaches to governing risk and risk management in organisations involve a combination of committees (Exhibit 2). Most commonly (68% of respondents) the governing body has established an Audit and Risk Committee to monitor governance, risk management and internal control throughout the organisation. Some governing bodies have set up distinct committees:

- An Audit Committee – established to monitor internal audit and external audit activity and overall governance; frequently supplemented by
- A Risk Committee – established to monitor management of risk by the management of the organisation.

Many organisations (30% of respondents) have set up executive-level committees to monitor the management of risk within the organisation.

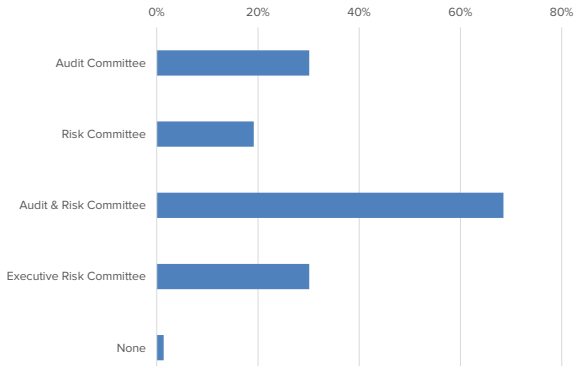

Exhibit 2 – Senior committees for governing risk

There is significant variation across industries in the use of dedicated risk committees or the establishment of both governance and executive committees for managing risk.

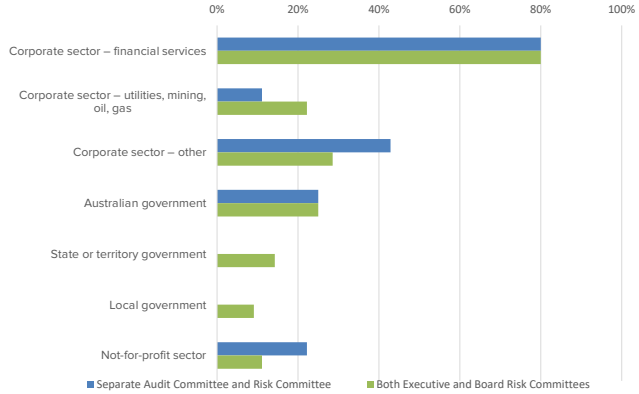

Exhibit 3 – Committees focusing on risk

Internal audit and Risk Management

To obtain a baseline understanding of arrangements, we asked whether internal audit and risk management were administratively distinct from each other within organisations. Where internal audit and risk management were different sections reporting to the same senior officer, they were assessed as being a joint function unless that senior officer was the chief executive officer. Slightly more than half of the responses indicated that risk management and internal audit had been set up as distinct functions within their organisations (See Exhibit 4).

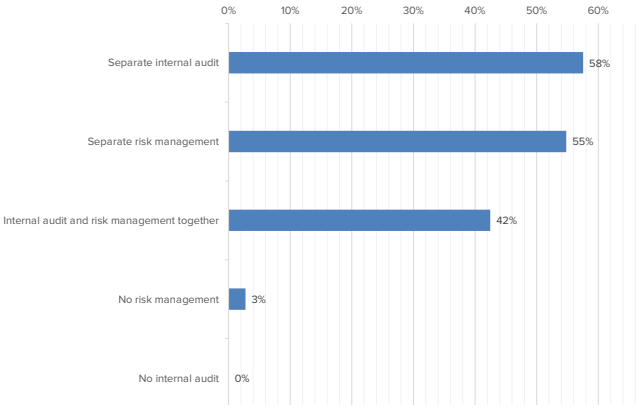

Exhibit 4 – Internal audit and risk management functions in organisations

The survey did not provide confidence that the decision to establish a joint function was based on a business case or conscious decision of the governing body.

To examine the arrangements for "joint" internal audit and risk management activities, we asked about administrative reporting arrangements (Exhibit 5). There are a number of combinations possible:

- The chief audit executive (CAE) being the manager of the chief risk officer(CRO)
- The CRO being the manager of the CAE
- The CAE and the CRO reporting to the same senior officer
- The CAE and the CRO being the same officer.

There is also a practice where the CRO and CAE both report to the chief executive officer but the CAE has an extra reporting line to the audit committee of the governing body.

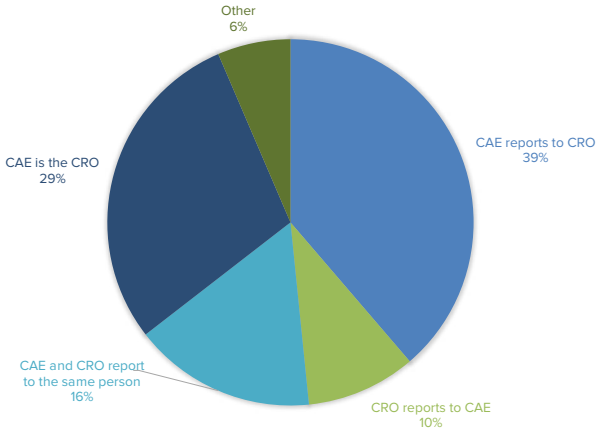

Exhibit 5 – Reporting lines

Independence and Objectivity Safeguards

A role of the internal audit function is to assess the controls in place to manage risks, to monitor the operation of controls, to test the reporting of risks to senior management and to audit the design and operation of the risk management framework. These roles complement the activities of the risk management function and provide assurance over the reporting from the function. It also involves assessment of matters for which the function is responsible. For this reason, mature organisations will wish to maintain their internal audit activity independently of the risk management function. This, however, is not always economically sensible.

Combining the two functions reduces the number of independent streams of information available to senior management and the governing body. ISO 37000 recommends that the governing body take advice separately from internal audit and risk management to strengthen their understanding of the organisation (Parkinson, 2021). Combining the functions has the potential to damage the organisation's operation by providing less comprehensive information to the governing body. In small organisations, the ability of senior management and the governing body to directly assess operations will reduce this damage.

Nevertheless, when the functions are operated jointly, there is need for safeguards to protect independence and objectivity. We asked about the use of a number of approaches to this problem (Exhibit 6).

Most joint functions had set up internal audit with reporting to an audit committee and/or with provisions in the internal audit charter to protect the independence of the internal audit function. These are both matters addressed in the Internal Auditing Standards (International Internal Auditing Standards Board, 2016).

1111 – DIRECT INTERACTION WITH THE BOARD

The chief audit executive must communicate and interact directly with the board.

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.

INTERPRETATION:

The chief audit executive may be asked to take on additional roles and responsibilities outside of internal auditing, such as responsibility for compliance or risk management activities. These roles and responsibilities may impair, or appear to impair, the organizational independence of the internal audit activity or the individual objectivity of the internal auditor. Safeguards are those oversight activities, often undertaken by the board, to address these potential impairments, and may include such activities as periodically evaluating reporting lines and responsibilities and developing alternative processes to obtain assurance related to the areas of additional responsibility.

Many organisations had made similar provisions in their management of the risk management function.

Exhibit 6 – Independence Safeguards

Of some concern are the 10% of relevant respondents who indicated that the joint function reported to a third rank executive – that is, to a person who reports to a deputy to the chief executive. We believe that this dilutes the three lines to the extent that flow of information may not

be reliable and leaves those charged with governance exposed. This is a matter that the audit committees of those organisations should address.

The ultimate test of independence is who is involved in assessing the performance of the head of the joint function. Exhibit 7 illustrates.

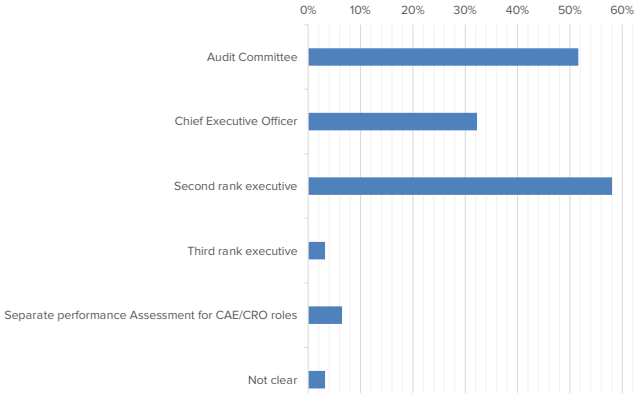

Exhibit 7 – Performance assessment of the joint function

In State and Australian government entities it is usual for the chief executive officer to be the governing entity of the organisation. There is no board, and the authority of a board is vested in the chief executive as the Accountable Authority. Of the ten respondents whose chief executive officer was involved in the assessment of the joint function, six of these chief executive officers were the Accountable Authority of the organisation. This demonstrates a healthy interest in the performance of the function.

About half of respondents had more than one entity involved in the performance assessment of the CAE. Pleasingly the assessment of the internal audit activities and of the risk management activities were done separately in some organisations even where the function was combined.

Of concern were those entities where there was a single assessor that was not the audit committee. As the audit committee is the recipient of functional reports from internal audit, the committee is the entity best placed to assess the performance the CAE.

- 10 (32% of joint functions) of the relevant respondents indicated that the performance of the CAE was assessed by a second rank executive only.
- 3 (10%) indicated that the assessment was by the audit committee alone. These were all organisations where the audit committee is a committee of the board.
- 3 (10%) reported that the assessment was done by the chief executive officer alone. One of these organisations was a government agency where the chief executive is the statutory governing body.

Summary

Risk Management and Internal Audit are both activities seeking to add value to their organisation and promote the efficient achievement of organisational objectives. They are different lines of information within the organisation and, ideally, are completely distinct.

Such a separation is sometimes impractical and nearly half of organisations responding to this survey maintain a joint function. The IIA would like to see mechanisms that help the two activities to maintain their independence from each other whilst cooperating where appropriate. This is promoted by the joint function reporting at a senior level of the organisation, having a strong relationship with the audit committee and being assessed on its risk management activities independently of the assessment of its internal audit activities.

Useful References

Cox, A. & Parkinson, M. J. A., 2023. Whitepaper: Internal Audit and Risk Management: Separate or Together?. [Online].

International Internal Auditing Standards Board, 2016. International Standards for the Professional Practice of Internal Auditing. [Online].

Parkinson, M. J. A., 2021. Elegant Alignment: ISO Guidance and the Three Lines Model. [Online]
Available at: https://www.theiia.org/en/content/communications/2021/october/global-knowledge-brief-from-the-iia-elegant-alignment-iso-guidance-and-the-three-lines-model/

The Institute of Internal Auditors - Australia, 2020. Factsheet: Risk Management. [Online].

The Institute of Internal Auditors - Australia, 2022a. Factsheet: Internal Audit and Risk Management Functions Working Together. [Online].

The Institute of Internal Auditors - Australia, 2022b. Factsheet: Internal Audit versus Risk Management. [Online].

The Institute of Internal Auditors, Inc, 2020. The IIA's Three Lines Model: an update of the three lines of defense. [Online]
Available at: https://www.theiia.org/en/content/position-papers/2020/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense/

The Institute of Internal Auditors, 2009. IIA Position Paper: The Role of Internal Auditing in Enterprise-wide Risk Management. [Online]
Available at: https://www.theiia.org/en/content/position-papers/2009/the-role-of-internal-auditing-in-enterprise-wide-risk-management/