

Institute of Internal Auditors - Australia (IIA-AU) Submission

*Proposed fifth edition of the Corporate Governance Council Principles
and Recommendations*

6th May 2024

Introduction

The Institute of Internal Auditors – Australia (IIA-AU) represents Governance, Risk and Control (GRC) professionals, particularly those working within an organisation to support the Board and Management. As a profession we have approx. 250,000 members world-wide in over 100 countries. With this clear focus, we limit our commentary to those areas where our members can best contribute expertise to support better governance outcomes for all stakeholders.

IIA-AU is a proud founding member of the ASX Corporate Governance Council and highly commends the work of the Council in developing this fifth edition of the *Corporate Governance Council Principles and Recommendations*. We are especially delighted to see the inclusion of the Global Internal Audit Standards – a benchmark in ethical and professional behaviour.

Unless stated otherwise, we support the Council’s position regarding the consultation questions.

Responses to Select Consultation Questions

Question 10

Recommendation 3.3: Does this new Recommendation appropriately balance the interests of security holders, other key stakeholders, and the listed entity? “A listed entity should have regard to the interests of the entity’s key stakeholders, including having processes for the entity to engage with them and to report material issues to the board.”

COMMENT: Broadly, we agree with the position put forward by the Council. However, this recommendation could be strengthened by including reference to the internal audit function including ‘Public Interest’ in their work as required under the new Global Internal Audit Standards released January 2024 with an effective date of January 2025.

The inclusion of Public Interest requires professional internal auditors to consider not only the interests of the board and security holders, but also the broader stakeholder groups, including society.

RECOMMENDATION IIA_1: In the commentary for Recommendation 3.3, include two additional bullet points under ‘The board’s activities may include, for example’:

Requiring the organisation’s Internal Audit plans to include assurance on the effectiveness of stakeholder relations activities, for achieving the entity’s strategic objectives

AND

Reviewing the ‘public interest’ findings and recommendations made by the organisation’s Chief Audit Executive

Both can reference the Global Internal Audit Standards.

Question 13

Recommendation 7.4: The Council is seeking to enhance the quality of existing reporting of material risks to an entity's business model and strategy, such as in the operating and financial review in its directors' report. Do you support the proposal that the entity identify and disclose its material risks, rather than identifying specific risks for all entities to disclose against?

COMMENT: We agree that an entity should identify and disclose its material risks. However, we also believe that this recommendation could be strengthened by including reference to using the internal audit function to identify and understand material risks.

The Obligations Hierarchy was the subject of a 2022 IIA Whitepaper which estimates that 38% of an organisation's obligations are statutory and regulatory (this is across all levels of government). The remaining 62% of obligations include:

- Business critical obligations.
- Essential obligations (Best practice, Standards and Contractual).
- Ethical obligations.
- Discretionary obligations (Asset maintenance and other deferrable items).
- Legacy obligations.

How an organisation performs on nearly two thirds of its obligations (doing what it says it will) falls outside regulation. This is where poor behaviour practices and potential scandal can arise. Internal Audit works across all areas of a business' obligations to give its board clarity and insight. It takes an organisation from compliance to performance.

RECOMMENDATION IIA_2: In the commentary for Recommendation 7.4, after the paragraph starting 'Listed entities should consider ongoing developments in sustainability...' add the following para graph:

Foresight into current and emerging risks may be derived from the work of an organisation's internal audit function, especially when that work is aligned with the business model and strategy. Working across structural, functional and category risks means that the internal audit function may have insights to enable organisations to more effectively assess current and emerging risks.

Question 18

Do you support an effective date for the Fifth Edition of the first reporting period commencing on or after 1 July 2025?

COMMENT: Yes, we support an effective date for the Fifth Edition of the first reporting period commencing on or after 1 July 2025, noting that the Global Internal Audit Standards come into effect January 2025.

Question 19

Do you wish to provide any other comments on the content of the Consultation Draft, including any other changes you would propose?

COMMENT: Thank you for this opportunity to share additional information. We wish to bring to the Council's attention an oversight that if addressed, we believe will assist the users of the document.

Limited understanding of internal audit. As the Council well knows, internal audit's name can create confusion with the better-known external auditing profession. But the functions are starkly different. An External Auditor provides an independent opinion on a company's financial statement and their conformance with accounting standards. It is focused on the past.

An Internal Auditor provides their organisation's governing body and management with independent, risk-based, and objective assurance across all its operations. In doing so, their purpose is to provide advice, insight, and foresight to strengthen the organisation's ability to create, protect, and sustain value. Unlike External Audit, the work is predominantly applied to bettering future performance.

Internal audit's role beyond the usual. In the majority, the recent and high profile public scandals relate to particular behaviours of organisations that reflect the culture of all or parts of the organisations. As referenced earlier, approximately 60% of an organisation's obligations – that is doing what it says it will do - falls outside regulation. Culture, or how we do what we do, sits squarely in the 60%. Culture cannot be regulated. Culture cannot be set by bathroom posters bearing values. Culture can, however, be observed.

Internal audit is part of a healthy and robust governance, risk management, and control processes framework. It provides vital independent information and insights on strategically important areas of risk so that informed decisions can be made. This includes cultural alignment with obligations and risk appetite. For this reason, APRA, through Prudential Standard CPS 220 Risk Management, requires the internal audit function report to the Board on the organisation's risk culture¹.

3-lines assurance model underpins GRC. The governing body of an organisation will seek assurance from management (line 1 assurance) and management may establish bodies to monitor and assist line management in performing their duties (line 2 assurance). For example, in many organisations, the role of the Chief Financial Officer is not to execute financial transactions, but rather to establish and monitor the financial management framework and to provide appropriate reporting and analysis. Similarly, the risk management function does not manage risks but rather establishes the framework and monitors, analyses, and reports on risk.

Internal audit is an assurance function (line 3 assurance) that reports directly to the governing body and provides information that is not influenced by the views of top management. This helps the board obtain a fuller view of operations and supports management in identifying opportunities and threats. Additionally, internal audit examines the activities of the line 2 assurance providers so that recipients of

¹ <https://www.apra.gov.au/sites/default/files/Prudential-Standard-CPS-220-Risk-Management-%28July-2017%29.pdf>

information from those activities (top management and the board) can be assured of the quality of that information.

Is internal audit a burden or a benefit? Rather than adding burden, internal audit helps businesses perform better. A competent internal audit function that is aligned to the organisation's objectives will provide advice and insight to improve decision-making which promotes the achievement of objectives and leads to more effective organisations.

Internal audit functions do not come without cost. Properly resourced internal audit functions require staff with relevant professional competence and tools to address the assurance needs of the organisation. However, the assurance services offered by internal audit provide those charged with the governance of organisations with information about the reliability of established systems and processes. This also promotes more effective organisations.

RECOMMENDATION IIA_3: Under the section headed 'Corporate Governance' reference the '3 Lines Model'² as an example of an internal assurance model that supports good corporate governance.

RECOMMENDATION IIA_4: In support of the *Corporate Governance Council Principles and Recommendations*, IIA-Australia strongly recommends and would equally support the Council providing a '3-line assurance model' education program for listed entities.

RECOMMENDATION IIA_5: Expand APRA's Prudential Standard CPS 220 Risk Management across all ASX listed entities so that the internal audit function will report to the Board on the organisation's risk culture.

² <https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf>

About Internal Audit GRC Professionals

Purpose

The purpose of internal audit is to strengthen an organisation's ability to create, protect, and sustain value by providing a governing body and management with independent, risk-based, and objective assurance, advice, insight, and foresight. Unlike External Audit, the work is predominantly applied to bettering future performance.

Standards of Professional Behaviour

As a profession, internal audit has some of the highest standards' thresholds including the function having its adherence to the standards independently reviewed with the assessment provided to the board.

Under the Global Internal Audit Standards that take effect January 2025, every Professional Member of IIA-AU is required to perform their duties with these behaviours embedded:

- With Integrity - requires honesty, but also professional courage to communicate necessary information even in difficult situations, and the ability to identify inappropriate corporate culture and its impacts.
- With Objectivity - objective in work performed and safeguarding that objectivity from real/perceived conflict of interest.
- With Due Care – competent, of course, and aligning the internal audit work with strategy governance, risk management and control processes, and applying professional scepticism to best serve the truthful flow of information.
- Confidentially with the Use of Information – information collected cannot be used for any other purpose.
- In the Public Interest – consider not only the interests of the governing body, but also stakeholders, including society.

Conclusion

Support

The IIA-AU thanks other members of the Council for the exemplary work. We support the adoption of this consultation draft in its entirety.

Recommendations

In addition to our support, we offer the following recommendations as outlined in the commentary of our submission.

RECOMMENDATION IIA_1: In the commentary for Recommendation 3.3, include two additional bullet points under 'The board's activities may include, for example':

Requiring the organisation's Internal Audit plans to include assurance on the effectiveness of stakeholder relations activities, for achieving the entity's strategic objectives

AND

Reviewing the 'public interest' findings and recommendations made by the organisation's Chief Audit Executive

Both can reference the Global Internal Audit Standards.

RECOMMENDATION IIA_2: In the commentary for Recommendation 7.4, after the paragraph starting 'Listed entities should consider ongoing developments in sustainability...' add the following paragraph:

Foresight into current and emerging risks may be derived from the work of an organisation's internal audit function, especially when that work is aligned with the business model and strategy. Working across structural, functional and category risks means that the internal audit function may have insights to enable organisations to more effectively assess current and emerging risks.

RECOMMENDATION IIA_3: Under the section headed ‘Corporate Governance’ reference the ‘3 Lines Model’³ as an example of an internal assurance model that supports good corporate governance.

RECOMMENDATION IIA_4: In support of the *Corporate Governance Council Principles and Recommendations*, IIA-Australia strongly recommends and would equally support the Council providing a ‘3-line assurance model’ education program for listed entities.

RECOMMENDATION IIA_5: Expand APRA’s Prudential Standard CPS 220 Risk Management across all ASX listed entities so that the internal audit function will report to the Board on the organisation’s risk culture.

³ <https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf>