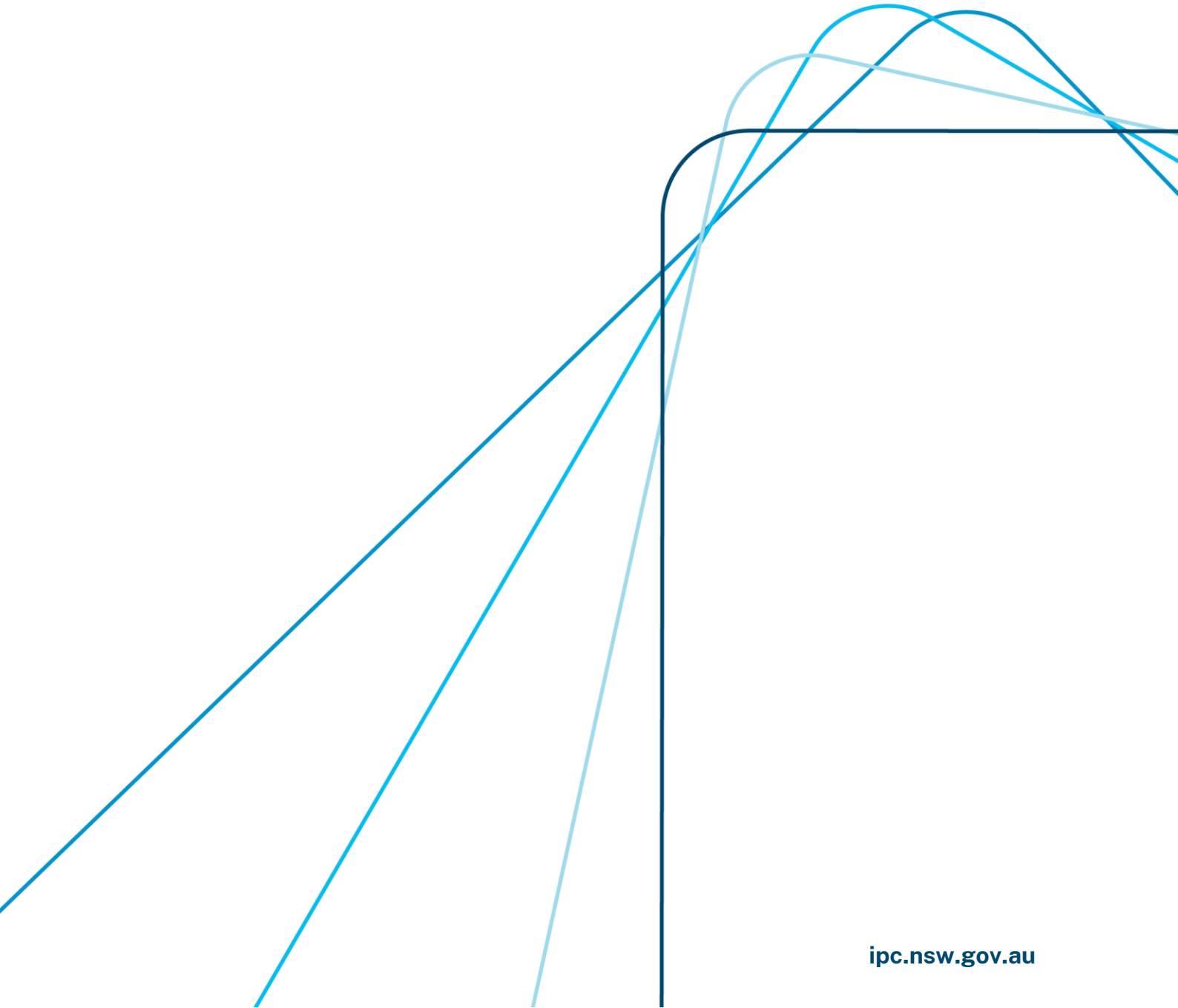
Information and Privacy Commission NSW

Audit and Risk Committee Charter 2025–26

November 2025



ipc.nsw.gov.au

Contents

1. Introduction 3

2. Objective 3

3. Authority 3

4. Composition & Tenure 3

5. Roles and Responsibilities 4

6. Responsibilities of Members 6

7. Reporting 7

8. Reporting Lines 7

9. Administrative Arrangements 8

10. Signatories 10

This Charter has been prepared to comply with TPP20-08 Internal Audit and Risk Management Policy for the General Government Sector

1. Introduction

The Chief Executive Officer/Information Commissioner (CEO) of the Information and Privacy Commission NSW (IPC) has established the Audit and Risk Committee (the Committee) in compliance with the *Internal Audit and Risk Management Policy for the General Government Sector* (TPP20-08).

The IPC satisfies the requirements of TPP20-08 to maintain a separate independent Audit and Risk Committee from the Department of Customer Service.[1]

This charter sets out the Committee's objectives, authority, composition and tenure, roles and responsibilities, reporting and administrative arrangements.

2. Objective

The objective of the Committee is to provide advice and independent assistance to the CEO by monitoring, reviewing and providing advice about the IPC's governance processes, risk management and control frameworks, and its external accountability obligations.

3. Authority

The CEO authorises the Committee, within the scope of its role and responsibilities, to:

- obtain any information it needs from any employee and/or external party (subject to their legal obligation to protect information)
- discuss any matters with the external auditor, or other external parties (subject to confidentiality considerations)
- request the attendance of any employee, including the CEO, at Committee meetings
- obtain external legal or other professional advice, as considered necessary to meet its responsibilities. The payment of costs for that advice by the agency is subject to the prior approval of the agency head.

4. Composition & Tenure

The Committee will consist of at least three (3) members, and no more than five (5) members[2] appointed by the CEO.

The CEO will appoint the Chair and members of the Committee. The Chair is counted as one of the members of the Committee.

Members will be appointed for an initial period no less than three (3) years and not exceeding five (5) years, after which they will be eligible for extension or re-appointment for a further term/s subject to a formal review of their performance (noting that the total term on the Committee will not exceed eight (8) years).

The Chair must be appointed for one (1) term only for a period of at least three (3) years, with a maximum period of five (5) years. The term of appointment for the Chair can be extended but any extension must not cause the total term to exceed five (5) years as a Chair of the Audit and Risk Committee.

Current employees of all NSW government sector agencies[3] other than State Owned Corporations cannot serve as members or Chairs of an Audit and Risk Committee.

---

[1] See Correspondence of 20 January 2021 from Chief Operating Officer, Department of Customer Service

[2] Inclusive of the Chair

[3] Government sector is defined in the *Government Sector Employment Act 2013*

The CEO and Chief Audit Executive (CAE) will not be members of the Committee but may attend as observers as determined by the Chair.

The members should collectively develop, possess and maintain a broad range of skills and experience relevant to the operations, governance and financial management of the IPC, the environment in which the IPC operates and the contribution that the Committee makes to the IPC. At least one member of the Committee must have accounting or related financial management experience with an understanding of accounting and auditing standards in a public sector environment.

5. Roles and Responsibilities

The Committee has no executive powers.

The Committee is directly responsible and accountable to the CEO, for the exercise of its responsibilities.

In carrying out its responsibilities, the Committee must at all times recognise that primary responsibility for management of the IPC rests with the CEO. The responsibilities of the Committee may be revised or expanded in consultation with, or as requested by, the CEO from time to time.

The Committee's responsibilities are to:

5.1 Risk Management

- Review whether management has in place a current and appropriate risk management framework that is consistent with *AS ISO 31000:2018*
- Assess and advise on the maturity of the IPC's risk management framework and risk culture
- Consider the adequacy and effectiveness of the internal control and risk management frameworks by reviewing reports from management, internal audit and external audit, and by monitoring management responses and actions to correct any noted deficiencies
- Review the impact of the IPC's risk management on its control environment and insurance arrangements
- Review the IPC's fraud and corruption control framework including the fraud control plan and be satisfied that the IPC has appropriate processes and systems in place to capture and effectively investigate fraud related information
- Seek assurance from management that emerging risks (including, but not limited to, climate risk and cyber risk) are being identified and addressed
- Seek assurance from management and Internal Audit that risk management processes are operating effectively, including that relevant internal control policies and procedures are in place and that these are periodically reviewed and updated
- Review whether a sound and effective approach has been followed in developing risk management plans for major projects, programs or undertakings
- Review whether a sound and effective approach has been followed in establishing the IPC's business continuity planning arrangements, including whether disaster recovery plans have been tested periodically.

5.2 Control Framework

- Review whether management's approach to maintaining an effective internal control framework, including over external parties such as contractors and advisors, is sound and effective

- Review whether management has in place relevant policies and procedures, and that these are periodically reviewed and updated
- Determine whether the appropriate processes are in place to assess, at least once a year, whether policies and procedures are complied with
- Review whether appropriate policies and procedures are in place for the management and exercise of delegations, at least annually, or whenever there are major changes that require a significant update to the manual
- Consider how management identifies any required changes to the design or implementation of internal controls
- Review whether management has taken steps to embed a culture which is committed to ethical and lawful behaviour
- Receive from management reports on all suspected and actual frauds, thefts and breaches of laws.

5.3 External Accountability

- Assess the policies and procedures for management review and consideration of the financial position and performance of the agency including the frequency and nature of that review (including the approach taken to addressing variances and budget risks)
- Review procedures around early close and year-end reporting
- Review the financial statements and provide advice to the CEO (including whether appropriate action has been taken in response to audit recommendations and adjustments), and recommend their signing by the CEO
- Satisfy itself that the financial statements are supported by appropriate management signoff on the statements
- Review the Chief Financial Officer Letter of Certification and supporting documentation (consistent with NSW Treasury Policy *CFO Certification on the Internal Control Framework over Financial Systems and Information* (TPG 24-08))
- Review cash management policies and procedures
- Review policies and procedures for collection, management and disbursement of grants and tied funding
- Review the processes in place designed to ensure that financial information included in the IPC's annual report is consistent with the signed financial statements
- Satisfy itself that the IPC appropriately measures and reports on its performance against objectives and State Outcomes.

5.4 Compliance and Ethics

- Determine whether management has appropriately considered legal and compliance risks as part of the IPC's risk assessment and management arrangements
- Review the effectiveness of the system for monitoring the IPC's compliance with applicable laws and regulations, and associated government policies
- Seek assurance that the appropriate exercise of delegations is monitored and reviewed
- Seek assurance that changes in key laws, regulations, internal policies and Accounting Standards affecting the agency's operations are being monitored at least once a year, and appropriately addressed
- Review the agency's process for communicating the code of conduct to staff and seek assurance as to compliance with the code

- Review policies and processes for identifying, analysing and addressing complaints
- Review whether management has taken steps to embed a culture which is committed to ethical and lawful behaviour.

5.5 Internal Audit

- Review and provide advice to the CEO on the internal audit policies and procedures
- Review the risk-based audit methodology
- Review the internal audit coverage and annual work plan, ensure the plan is based on the IPC's risk management plan, and recommend approval of the plan by the CEO
- Advise the CEO on the adequacy of internal audit resources to carry out its responsibilities, including completion of the approved internal audit plan
- Review audit findings and related recommendations, particularly those that have been assessed as high risk if audit finding recommendations are not implemented
- Provide advice to the CEO on significant issues identified in audit reports and action taken on these issues, including identification and dissemination of good practice
- Monitor management's implementation of internal audit recommendations
- Review and endorse the internal audit charter including ensuring appropriate agency structures, authority, access to senior management and reporting arrangements are in place
- Assess the overall effectiveness and evaluate the performance of the CAE and internal audit function
- Committee Chair to contribute to the CAE's regular performance review
- Provide advice to the CEO on the results of any external assessments of the internal audit function
- Provide advice to the CEO on the appointment or replacement of the CAE and recommend to the CEO the appointment or replacement of external internal audit service providers (in the case of an outsourced internal audit function).

5.6 External Audit

- Act as a forum for communication between the CEO, senior management and internal and external audit
- Provide feedback on the financial audit coverage proposed by external audit and be informed of planned performance audit scope prior to their commencement
- Review all external plans and reports (including management letters) in respect of planned or completed audits and monitor management's implementation of audit recommendations.

6. Responsibilities of Members

Members of the Committee are expected to understand and observe the requirements of the Internal Audit and Risk Management Policy (TPP 20-08). Members are also expected to:

- Make themselves available as required to attend and participate in meetings
- Contribute the time needed to study and understand the papers provided
- Apply good analytical skills, objectivity and good judgement

- Abide by the relevant ethical codes that apply to employment within the General Government Sector
- Express opinions frankly, ask questions that go to the fundamental core of the issue and pursue independent lines of enquiry
- Maintain strict confidentiality, even after their terms on the Committee end, and declare any real or perceived conflicts of interest proactively and promptly.

7. Reporting

The Committee will regularly, but at least once a year, report to the CEO on its operation and activities during the year. The report should include:

- An overall assessment of the IPC's risk, control and compliance framework, including details of any significant emerging risks or legislative changes impacting the IPC
- A summary of the work the Committee performed to fully discharge its responsibilities during the preceding year
- Details of meetings, including the number of meetings held during the relevant period, and the number of meetings each member attended
- A summary of the IPC's progress in addressing the findings and recommendations made in internal and external reports
- A summary of the Committee's assessment of the performance of internal audit.

The Committee may, at any time, report to the CEO any other matter it deems of sufficient importance to do so. In addition, at any time an individual committee member may request a meeting with the CEO.

8. Reporting Lines

The Committee must at all times ensures it maintains a direct reporting line to and from internal audit and act as a mechanism for internal audit to report to the CEO on functional matters.

The IPCs' reporting line is prescribed in Figure 1.

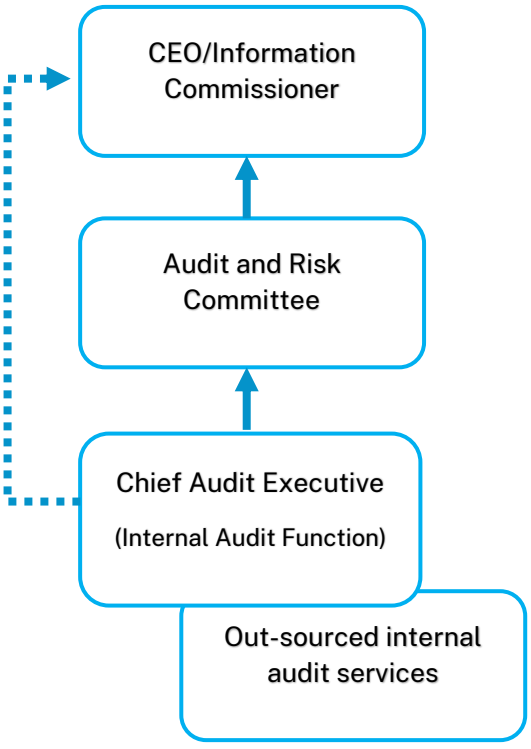


Figure 1 Reporting Lines

9. Administrative Arrangements

9.1 Meetings

The Committee will meet at least four (4) times per year. A special meeting may be held to review the IPC's annual financial statements.

The Chair is required to call a meeting if requested to do so by the CEO, or another Committee member.

A meeting plan, including meeting dates and agenda items, will be agreed by the Committee and the IPC at the beginning of each calendar year. The estimated total remuneration per Independent Chair and Member will be determined based on the estimated number of meetings and monitored by the agency. The meeting plan will cover all the Committee's responsibilities as detailed in this Charter.

The Committee may deal with matters out of session as appropriate including by email, teleconference or in person. Minutes of any matters the Committee addresses out of session will be maintained by the Committee Secretariat. Matters may be separately minuted or recorded in the minutes of the next formal meeting.

9.2 Attendance at Meetings & Quorums

A quorum will consist of a majority of Committee members. A quorum must include at least two (2) independent members.

Meetings can be held in person, by telephone or by video conference.

The CEO may attend the meetings of the Audit and Risk Committee. Committee members, if necessary, are able to have in-camera discussions. The CAE, external audit representatives and any other agency representatives may attend Committee meetings, except where the Committee members wish to have in-camera discussions. The Committee may also request the Director, Finance (Department of Customer Service) or other employees attend committee meetings or participate for certain agenda items.

All attendees are responsible and accountable for maintaining the confidentiality of the information they receive during the course of these meetings.

The Committee is required to meet separately with both the internal and external auditors at least once a year.

9.3 Dispute Resolution

Members of the Committee and the IPC's management should maintain an effective working relationship and seek to resolve differences by way of open negotiation. However, in the event of a disagreement between the Committee and management (including the CEO), the Chair may, as a last resort, refer the matter to NSW Treasury to be dealt with independently.

9.4 Secretariat

The CEO will appoint a person to provide secretariat support to the Committee. The Secretariat will ensure the agenda and supporting papers are circulated, after approval from the Chair, at least one (1) week before the meeting, and ensure the minutes of the meetings are prepared and maintained.

Minutes shall be approved by the Chair and circulated by the Secretariat within two (2) weeks of the meeting to each member and committee observer, as appropriate.

9.5 Maintenance of Records

The Secretariat shall maintain records of all meeting papers and minutes, the Committee's key functional and administrative arrangements (remuneration, reappointment, conflict of interest declarations, etc.), reviews of the Committee and its Charter, and any other material relevant to the conduct of the Committee and its meetings.

9.6 Conflicts of Interest

Once a year the Committee members will provide written declarations to the CEO stating they do not have any conflicts of interest (perceived, actual or potential) that would preclude them from being members of the Committee.

Committee members must declare any conflicts of interest at the start of each meeting or before discussion of the relevant agenda item or topic. Details of any conflict of interest should be appropriately minuted.

Any external provider of internal audit services must also declare any conflicts of interest at the start of each meeting or before discussion of the relevant agenda topic. Details of any conflict of interest should be appropriately minuted.

Where members or observers at the committee meetings are deemed to have a perceived, actual or potential, conflict of interest, the Chair (or a quorum of the Committee if the conflict of interest arises from the Chair) may excuse them from Committee deliberations on the issue where a conflict of interest exists.

As the Chief Audit Executive (CAE) carries responsibilities for other activities, in circumstances where an Internal Audit activity is in the business area of the CAE, the Director Business Improvement will oversight the Internal Audit engagement.

9.7 Induction

New members will receive relevant information and briefing on their appointment to assist them to meet their committee responsibilities.

9.8 Assessment Arrangements

The CEO, in consultation with the Chair of the Committee, will establish a mechanism to review and report on the performance of the Committee, including the performance of the Chair and each member, at least annually.

The review will be conducted on a self-assessment basis (unless otherwise determined by the CEO) with appropriate input sought from the CEO, the internal and external auditors, management and any other relevant stakeholders as determined by the CEO.

9.9 Review of Charter

At least once a year the Committee will review this Charter. This review will include consultation with the CEO.

Any substantive changes to this Charter will be recommended by the Committee and formally approved by the CEO.

10. Signatories

Chief Audit Executive

Rachel Jhinku

Name

Signature

Date

CEO/Information Commissioner

Rosalind Croucher

Name

Signature

Date

Chair of Audit and Risk Committee

Peter Scarlett

Name

Signature

Date

Document information

Identifier/Title:	Audit and Risk Committee Charter
Business Unit:	IPC
Author:	Chief Audit Executive
Approver:	CEO
Date of Effect:	November 2025
Next Review Date:	September 2026
EDRMS File Reference:	D20/053376/DJ
Key Words:	audit, internal review, governance, risk management, fraud, performance

Document history

Version	Date	Reason for Amendment
1.0	October 2018	Initial Draft – review of policy
1.0	November 2019	ARC and CEO feedback incorporated
1.0	November 2020	Minor revisions
1.0	December 2020	Minor revisions approved by ARC
1.1	March 2021	Revision to include IPC separate status of ARC
1.2	September 2021	Revisions to align with TPP20-08 requirements
1.3	September 2022	Annual Review and revisions for QAIP Review
1.4	September 2024	Annual Review
1.5	September 2025	Annual Review

Information and Privacy Commission NSW
T 1800 IPC NSW (1800 472 679)
www.ipc.nsw.gov.au

Information and Privacy Commission NSW