audit office
OF NEW SOUTH WALES

Compliance Policy

Version: 4.0

Date: 12 August 2024

Review date: August 2027

contents

1. Policy statement

The Audit Office of New South Wales (the Audit Office) is a statutory authority with significant compliance obligations from laws and regulations, central agency directions, professional standards and codes. The Audit Office's core business is principally conducted under the *Government Sector Audit Act 1983* and the *Local Government Act 1993*. The *Government Sector Finance Act 2018* and Regulation, which establishes a framework for public sector financial and resource management, also set out key obligations and minimum standards for the Audit Office.

The Audit Office must conduct its business and activities in a lawful and responsible way. The Audit Office aims to drive compliance through its culture and values, as well as by:

- understanding and managing compliance risks
- assigning responsibility for meeting specific compliance obligations
- requiring all staff to meet their compliance obligations within the scope of their role, function, authority and span of control
- assessing and improving compliance performance.

The Audit Office is committed to the continuous improvement of its compliance management system.

2. Policy objective

This Compliance Policy sets out the Audit Office's approach to compliance and the management of compliance risk through a set of guiding principles and the components of our risk-based compliance management system.

This Policy provides a framework for managing compliance obligations and outlines how the Audit Office identifies, monitors, and manages compliance obligations, and guides staff on their responsibilities and expectations. The policy also seeks to promote a sustainable compliance framework, that is flexible and responsive to change.

3. Policy scope

This Policy applies to:

- all staff within the scope of their role, function, authority and span of control
- all functions and business activities, both corporate and audit related
- all compliance obligations, those we must and choose to comply with.

This Policy should be read in conjunction with individual Audit Office policies covering specific areas or activities. See section 9 for definitions of 'staff' and 'compliance obligations'.

4. Risk appetite statement

The Audit Office is committed to compliance with relevant legislation, regulation, professional obligations as well as internal policies. We have a low-risk appetite for non-compliance that could impact our reputation or ability to operate. We recognise that compliance risks exist despite our best efforts, however the Audit Office has no appetite for deliberate or purposeful breaches of legislative, regulatory, professional or critical internal policy obligations. It expects all activities to be conducted in a lawful and responsible way.

We proactively monitor changes in our compliance obligations to ensure timely adjustments with the aim to mitigate non-compliance risks promptly and effectively. Identified compliance breaches must be reported and remedied as soon as practicable.

5. Compliance principles

It is expected that staff are guided by the following principles when carrying out responsibilities and activities within their scope of their role, function, authority and span of control.

Principle	Expectation
Ethical and lawful	• activities will be lawful and responsible, aligned to the highest standards, and will support staff to remain up to date with new or changes to existing compliance obligations • compliance expectations, conduct and behaviour of staff, will be in accordance with the Audit Office's values and the Code of Conduct.
Accountable and transparent	• all staff are to adhere to the Audit Office's policies, procedures and processes, and the compliance obligations within the scope of their role, function, authority and span of control, and will report non-compliance where required. • compliance expectations will be clearly explained to staff, and effective monitoring, evaluation and learning will be embraced – this includes protecting and valuing the reporting of compliance concerns and failures, including instances of non-compliance made in good faith.
Collaborative and proactive	• compliance activities will be undertaken collaboratively within and across teams, and with other stakeholders such as integrity agencies or other government agencies as relevant, to achieve an effective compliance management system. • timely awareness of new or changes to existing compliance obligations will be ensured, and steps taken to prepare for changed processes or activities to ensure compliance within required timeframes – this includes attending relevant training or seeking information as required.
Proportionate and risk based	• compliance activities will be given priority in those areas that pose the greatest risk and corrective action taken proportionately to the level of non-compliance or risks to non-compliance. • corrective action, including any disciplinary action, will be proportionate to the level of risk posed and the seriousness of the non-compliance and the culpability of the person(s) involved.

6. Roles and responsibilities

Role	Responsibilities
Auditor-General	The Auditor-General is ultimately responsible for the Audit Office's compliance management system and ensuring adequate resources are allocated to meet compliance obligations.
Office Executive (OE)	The OE assist the Auditor-General to meet their statutory responsibilities and provide leadership to the Audit Office. This includes responsibility for: • monitoring compliance risks and ensuring any significant non-compliance is being managed and corrective action is taken • monitoring the periodic review of key policies, and reviewing and approving key policies as detailed in the Policy Register • promoting a compliance culture. Refer to the OE Charter for further details.
Audit and Risk Committee (ARC)	The ARC independently reviews the Audit Office's compliance management system and management of compliance risks in accordance with the current NSW Treasury Internal Audit and Risk Management Policy for the General Government Sector by:

Role	Responsibilities
	• determining whether management has appropriately considered legal and compliance risks as part of the Audit Office's compliance risk assessment and management arrangements • reviewing the effectiveness of systems for monitoring the Audit Office's compliance with applicable laws and regulations, and associated government policies. Refer to the ARC Charter for further details.
Executive Director, Professional Services	The ED – Professional Services oversees the maintenance and continuous improvement of the compliance management system, including oversight, strategic direction and support for the activities undertaken by the Governance and Quality & Technical units. The ED – Professional Services also has authority to seek a general legal opinion.
Governance unit - compliance function, Professional Services Branch *Led by the relevant director in the Governance unit (currently Director, Legislation & Assurance), and supported by the Governance Manager and Governance Officer.*	The compliance function within the Governance unit is responsible for the effective operation of the Audit Office's compliance management system, including by: • facilitating the identification of compliance obligations, including updating the Compliance Risk Register for new, or changes to existing, legislative obligations • providing advice and guidance on the compliance management system and compliance obligations, including coordinating external legal advice. • coordinating the annual compliance review, including the compliance risk assessment • maintaining a compliance reporting system, and a system for raising concerns including internal Public Interest Disclosures • planning and coordinating the internal audit program to identify compliance risks and gaps • monitoring and measuring compliance performance, including analysing and evaluating the performance of the compliance management system to identify any need for corrective action • ensuring the compliance management system is reviewed at planned intervals • reporting to the OE and the ARC (see section 7.2 for further details). The compliance function also supports compliance obligation owners to ensure that: • responsibilities to achieve compliance obligations are appropriately allocated throughout the Audit Office • compliance obligations are integrated into policies, processes and procedures • all relevant staff are trained as required • compliance performance indicators are established.
Quality and Technical unit, Professional Services Branch	Relevant staff in the Quality & Technical unit are responsible for: • reviewing changes to legislation and other pronouncements likely to impact Financial and Performance Audit Branches and the Audit Office more broadly • informing responsible compliance or policy owners of any implications found in these reviews • providing advice and guidance to the Audit Office on compliance matters • overseeing compliance through quality assurance activities • maintaining, researching and disseminating technical information, including changes in legislation and pronouncements by standard setters, regulators and professional bodies • ensuring that the Crown Solicitor's Opinions (CSO) register is maintained.

Role	Responsibilities
Compliance obligation owners *Typically directors or managers ('senior management'), who are assigned operational responsibility for managing and implementing relevant compliance obligations.*	Compliance obligation owners should lead a compliance culture and set an example in meeting all compliance obligations. They are also specifically responsible for: • monitoring compliance with relevant obligations in their area of responsibility • identifying, understanding and responding to new compliance obligations, and integrating these into policies, procedures and practices • ensuring controls are designed, implemented and in place to minimise the risk of non-compliance • monitoring staff awareness of obligations, taking steps to build awareness and directing staff to meet training requirements where applicable • identifying whether exception reporting is applicable for their obligations, and embedding relevant exception reporting within respective policies • providing a compliance status update for their area as part of the annual compliance review conducted by Governance.
Managers *including people managers*	Managers should lead an effective compliance culture within their teams and set an example in meeting compliance obligations. They are also responsible for: • ensuring compliance with the Audit Office's obligations, policies, procedures and processes within their area of responsibility and with obligations relevant to their teams • identifying and communicating compliance risks in their operations • encouraging their staff to raise compliance concerns • actively participating in the management and resolution of compliance incidents and ensuring appropriate corrective action is implemented, including escalating any unresolved or significant issues as required.
All staff	Must adhere to the Audit Office's compliance policies, procedures and processes, and the relevant compliance obligations within the scope of their role, function, authority and span of control. This includes being guided by the compliance principles, outlined in section 5 and participating in relevant training or seeking information as required. All staff must report compliance concerns, issues, and failures, including instances of non-compliance to their manager.

7. Compliance management system

The Audit Office's compliance management system covers the compliance obligations the Audit Office has to, and chooses to, comply with as part of its corporate and audit functions.

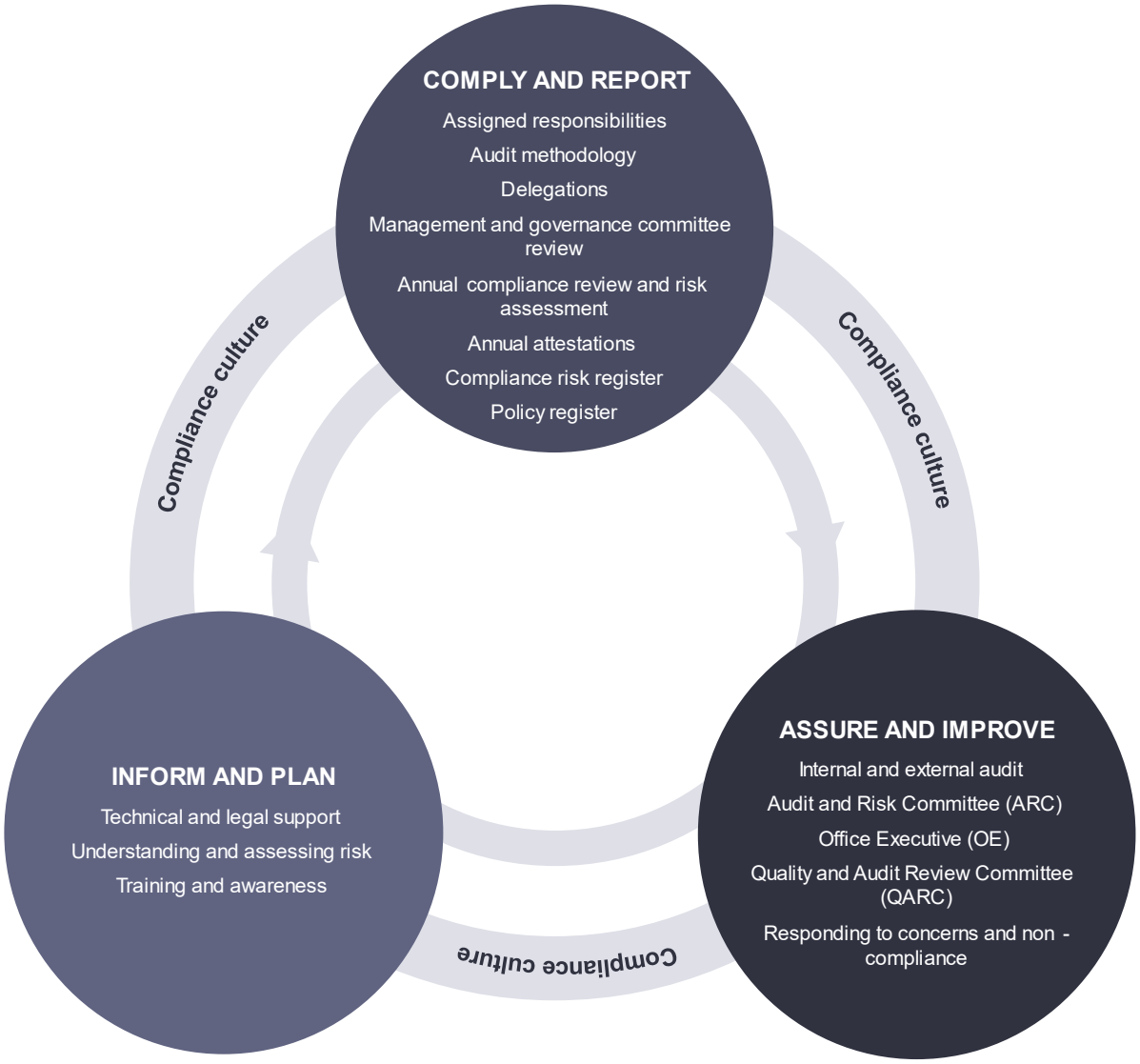
Our compliance management system helps us:

- identify new or changes to existing compliance obligations
- comply with compliance obligations
- prevent, identify and respond to non-compliance
- promote a culture of compliance.

Compliance culture is the values, ethics, beliefs and conduct that exist throughout the Audit Office and interact with the Audit Office's structures and control systems to produce behavioral norms that are conducive to compliance. The compliance principles outlined in section 5 of this policy reflect and support the compliance culture.

Components of the Audit Office's compliance management system

The Audit Office's compliance management system promotes the importance of compliance to all staff. Key components of our compliance management system include:



7.1 Inform and plan

Technical and legal support

Identifying and evaluating new or changed compliance obligations, and planning for their implementation, is the responsibility of compliance obligation owners. This typically involves:

- reviewing legislation websites, and the websites of professional bodies and central agencies, and forwarding this information to relevant staff for action
- regularly conducting environmental scans, including issues reported in the public and private sector or in media and discussions at networking or training events.

This process is supported by the Governance unit, with respect to corporate compliance, and by the Quality & Technical unit, with respect to audit and accounting standard compliance. External legal advice can be sought, if required, through the Professional Services Branch.

Understanding and assessing risk

Compliance obligations owners need to understand and assess relevant compliance risks. The Chief Risk Officer, who leads the Audit Office's Risk Management Function, can provide advice on and challenge the management of risk and control effectiveness.

Training and awareness

The need for training and awareness-raising should be identified by compliance obligation owners, and is supported by:

- the Learning and Development program: induction and ongoing training, audit methodology, professional updates, and targeted training to ensure staff meet obligations within the scope of their role, function, authority and span of control
- communication or notifications to staff of new or changes to existing obligations and on the job training.

7.2 Comply and report

Assigned responsibilities are the responsibilities captured in position descriptions, individual performance agreements and in individual Audit Office policies.

Audit methodology is aligned to and ensures compliance with professional standards.

Delegations

- The Delegations Manual is maintained by Finance and Performance Branch to establish the levels of authority delegated by the Auditor-General to duly appointed office holders and staff.
- Statutory delegation instruments maintained by the Professional Services Branch which delegate functions conferred or imposed on the Auditor-General by various legislation.

Management and committee review

Management and committee review supports the identification of risks and provides for a second line of internal control. This involves:

- management reviewing and monitoring compliance activities designed to meet compliance obligations within their area of responsibility
- internal assessments or reviews of management activities performed by other committees, generally led by a member of the Office Executive.

Refer to the respective committee charters for further details.

Annual compliance review and risk assessment

The compliance review is conducted annually (or more frequently if required) and coordinated by the compliance function in the Governance unit. It requires the compliance obligation and policy owners to check their compliance obligations and policies, provide input, complete the attestation and update the compliance risk register and policy register if required.

The compliance risk assessment is conducted simultaneously with the annual compliance review and in line with the Audit Office's Risk Management Framework. The risks of non-compliance are monitored, and effective internal controls put in place to reduce compliance risks to an acceptable level.

MiIntegrity is used to facilitate status updates of compliance obligations. The system assists in ensuring that information about compliance obligations is complete, accurate and up to date.

Annual attestations

Attestations play a key role in reviewing and confirming key compliance requirements. These include:

- compliance obligation and policy attestations, which are completed annually by compliance obligation owners to confirm compliance with the Audit Office policies, and coordinated by the compliance function in the Governance unit as part of the annual compliance review
- other annual declarations, such as the management control questionnaire, Code of Conduct sign-off, conflict of interest attestation, compliance with current NSW Treasury Policy Internal Audit and Risk Management Policy for the General Government Sector, System of Quality Management attestation and the NSW Cyber Security Policy.

Reporting

The compliance function within the Governance unit is responsible for reporting to the OE and the ARC on the effectiveness of the compliance management system. This includes reporting about:

- the results of annual compliance review and the risk assessment
- compliance performance of the compliance management system
- completion rates of the annual Code of Conduct sign-off and conflict of interest annual attestation
- any significant non-compliance and
- actions taken to minimise the risks of non-compliance to acceptable levels.

Exceptions reporting

Compliance obligation owners are responsible for identifying whether exception reporting (i.e., reporting on compliance breaches/non-compliance) is applicable, and if relevant, embedding the exception reporting within the respective policies. Compliance obligation owners report any exceptions related to their compliance obligations to the OE as required.

Compliance indicators

Compliance indicators can assist in evaluating the achievement of our compliance objectives and assessing our compliance performance. Indicators that are used by compliance obligation owners and/ or the Governance unit, as relevant, include:

- results of the compliance risk assessment, which identifies emerging risks and ensures that risk mitigation strategies are targeted and effective
- compulsory compliance-related training, including its frequency, completion rates and post-training test results
- currency of internal policies (including the Code of Conduct), and frequency of review and update of internal policies
- findings from internal and external audits that evaluate adherence to regulatory requirements and internal policies, and data on implementation of recommendations
- employee survey results, internal and external, including survey questions that relate to our values and compliance culture
- exceptions reported, such as policy breaches and other non-compliance, including number and nature of incidents
- public interest disclosures and complaints received about the Audit Office.

7.3 Assure and improve

The compliance management system needs to be suitable, adequate and effective. To achieve this, assurance and continuous improvement are done by:

- leveraging the ARC members' experience and feedback about the effectiveness of the compliance management system and whether the Audit Office has appropriately considered legal and compliance risks
- internal audit review of the compliance management system and compliance to specific legislation and Audit Office policies
- implementing the recommendations from internal and external audit and other independent reviews of the Audit Office, and completing the annual quality review of the internal audit function
- engaging with the CRO to understand how the Audit Office's operating environment may be impacting on compliance risks, and how compliance risks impact other organizational risks
- drawing upon the outcomes of investigations, including identifying the root causes of non-compliance and making the relevant improvements based on the lessons learned
- implementing recommendations arising from internal quality reviews completed by QARC (refer to the QARC Charter for further details)
- considering compliance issues from a systemic perspective raised in any complaints and public interest disclosures about the Audit Office
- assessing feedback from auditees, staff and regulators
- evaluating the feedback from training and awareness activities.

Responding to concerns and non-compliance

The Audit Office adopts a proportionate and risk-based approach to non-compliance and treats all reports of non-compliance seriously.

Staff are encouraged and required to report to management compliance concerns, issues and failures and should do so without fear of retaliation (refer to the Internal Public Interest Disclosure Policy for further details about how to report concerns of wrongdoing by staff). Non-compliance by staff will be dealt with appropriately and corrective action taken as required, in line with the relevant People & Culture policies,[1] and the Internal PID Policy where appropriate.

Organisational non-compliance identified through assurance, audit and review processes are reported to the OE and ARC, and the implementation of management actions to address these is overseen by the Chief Audit Executive. This provides assurance around remedial actions to address concerns about the adequacy of the systems and processes to ensure future compliance.

8. Legislative context

This Policy has been developed in line with the Australian standard *AS ISO 37301:2023 Compliance Management Systems – Requirements with guidance for use*.

Other relevant documents that were considered include:

- NSW Treasury Policy: Internal Audit and Risk Management Policy for the General Government Sector
- Guide for Audit & Risk Committees: Compliance Management, NSW Treasury
- AS ISO 31000:2018 Risk management – Guidelines
- NSW Treasury Risk Management Toolkit for NSW Public Sector Agencies
- APES 110 Code of Ethics for Professional Accountants
- Audit Office's Risk Management Framework
- other Audit Office's policies, registers and charters

[1] For example, the Performance Management Policy, Grievance Policy or Disciplinary Policy.

9. Definitions

In the context of this Policy and in line with AS ISO 37301:2023:

Audit Office of NSW is used for initial reference in the Policy and thereafter referred to as the Audit Office.

Compliance culture is the values, ethics, beliefs and conduct that exist throughout the Audit Office and interact with the Audit Office's structures and control systems to produce behavioral norms that are conducive to compliance.

Compliance obligations are the requirements that the Audit Office:

- has to comply with, such as relevant legislation, regulations, central agency directions, industry and organisational standards and codes, requirements for certain certifications, government policies, contracts, professional standards, etc.
- chooses to comply with, such as internal policies and frameworks, codes of conduct, better practice, accepted community and ethical standards etc.

Compliance obligation owner is the position/title/role within the Audit Office assigned to staff that have a specific duty or task to manage a particular compliance obligation**.**

Compliance management system refers to interrelated or interacting elements of the Audit Office to establish policies, objectives and processes, including the Audit Office's structure, roles and responsibilities, and planning and operations, to achieve compliance objectives.

Compliance risk is the effect of uncertainty on compliance objectives. It is expressed in the terms of a combination of the consequence of non-compliance with the Audit Office's compliance obligations and the associated likelihood of occurrence.

Compliance risk register is a list of the Audit Office's key compliance obligations, hosted in MiIntegrity. Each obligation is risk assessed and is assigned a responsible compliance obligation owner to ensure compliance with the obligation.

Contingent workers refer to staff who are employed through a recruitment agency.

Continual improvement means any recurring activity to enhance performance.

Corrective action is an action to eliminate the cause(s) of a non-conformity and to prevent recurrence.

Employee refers to persons employed by the Audit Office under Award or Executive Contract conditions of employment.

Non-compliance refers to non-fulfilment of compliance obligations.

Policy register is a register of key Audit Office policies, policy owners, policy review dates, and legal obligations covered by a policy.

Responsibilities refer to the activities or outcomes that someone is responsible for performing directly, or ensuring are delivered. Responsibilities often include activities such as 'approving', 'reviewing', 'monitoring', 'implementing' and 'communicating'.

Risk management is the identification, analysis, assessment and evaluation of risks and opportunities and is built into everything we do, especially in informing our decisions. The objective is to reduce the impact of risks while realising opportunities to ensuring our overall objectives are met.

Staff or staff member includes all Audit Office employees (that is persons employed under the Award conditions or on executive contract), and contingent workers. Contingent workers are staff who are employed through a recruitment agency.

10. Implementation procedures and related policies

Other core policies related to this Policy include the:

- Policy Framework
- Code of Conduct
- Statement of Business Ethics
- Conflict of Interest and Professional Independence Policy
- Fraud and Corruption Control Policy
- System of Quality Management
- Risk Management Framework
- Internal Public Interest Disclosure Policy.

11. Contact point

If staff have any questions about this Policy, they should contact the Director, Legislation and Assurance, or the Governance unit via governance@audit.nsw.gov.au.

12. Review

This Policy will be reviewed every three years or earlier if any significant new information, legislative or organisational change warrants an update in this document.

Document information

Title:	Compliance Policy
Owner:	Governance
Person responsible:	Executive Director, Professional Services
Approver:	Office Executive
Last updated:	12/08/2024
Next review date:	08/2027
Document reference:	R012-728983147-32151

Document history

Version	Date	Reason for amendment
4.0	July 2024	Review and update to reflect current Audit Office branch structure, changes to role titles, and references to new Audit Office policies. Additions include a risk appetite statement and diagram to visually represent our compliance management system. Other changes and refinements made to enhance alignment with the relevant standard.