Office of Sport

Compliance Management Policy and Procedure

April-2023

Summary

All employees must understand and comply with relevant compliance obligations (including policies and procedures) and report suspected breaches. All leaders must resource compliance and lead a compliance culture. Managers must identify, escalate and improve compliance with key obligations in their area and ensure their employees are provided access, awareness, training and communication on compliance responsibilities. Owners and Responsible Officers must ensure the contents of the Compliance Management Register are current and accurate. Managers must ensure compliance breaches are identified, documented, treated, escalated and reported. This document should be read in conjunction with the Compliance Management Framework.

Document information

Title:	Compliance Management Policy and Procedure
Version:	v1.2
Approved date:	19 April 2023
Approver:	Chief Executive
Owner:	Manager, Audit, Risk & Governance
Contact:	Manager, Audit, Risk & Governance
Publishing:	This document can be published on the intranet and internet
Review:	Every 4 years
Next Review:	April 2027
Related Documents and Forms:	Compliance Management Register (Smartsheet link)
Related Internal Policies/Procedures:	Compliance Management Framework Enterprise Risk Management Framework, Policy and Procedures Public Interest Disclosure Policy and Procedure Code of Conduct and Ethics
Related External Policies or Links:	Public Service Commission: The Code of Ethics and Conduct for NSW government sector employees AS ISO 37301:2023 Compliance management systems — Requirements with guidance for use ISO 37000:2021 Governance of organizations – Guidance ISO 37002:2021 Whistleblowing management systems — Guidelines AS ISO 31000:2018 Risk Management - Guidelines. TPP 20-08 Internal Audit and Risk Management Policy for the General Government Sector. *Public Interest Disclosures Act 2022*

Version	Amendments**	Prepared by title, unit	Date	Record No.
v1.0	Initial release: CE approved 28-Jan-16	Manager, Audit, Risk & Governance	28 January 2016	CDOC15/42894
v1.1	Minor administrative amendments, policy link updates and document format change.	Manager, Audit, Risk & Governance	1 March 2019	D19/20086
v1.2	Minor administrative amendments, policy link updates and document format change to new template. CE approval 19-April -23	Manager, Audit, Risk & Governance	19 April 2023	D23/26520

Table of contents

Policy

1 Policy Statement

The Office of Sport (OoS) is committed to complying with all key obligations. This includes legislative obligations, regulatory policies, government requirements, industry codes and standards, as well as OoS policies, procedures and *The Code of Ethics and Conduct for NSW government sector employees* (Code of Conduct).

To facilitate this, the OoS has developed a compliance management system which is described in the *Compliance Management Framework* (the framework). This policy is an element of the framework.

The establishment and integration of this framework will help to ensure OoS operations are in accord with key compliance obligations; a compliance culture is promoted, and corporate governance practices are supported.

The framework enables the OoS to:

- meet its compliance obligations by assigning responsibility and preventing, identifying and responding to noncompliance where necessary,
- manage its compliance risk,
- conduct its business and activities in a lawful and responsible way, and
- achieve its objectives through integration of compliance management with all OoS operations.

2 Scope

Applies to all OoS employees, it should be read in conjunction with the *Compliance Management Framework*.

3 Definitions

Term	Definition
Compliance	For the purposes of this document, 'compliance' is defined as adhering to the requirements of laws, regulations, central agency directions, industry and organisational standards and codes, and principles of good governance.
Compliance Management Framework	A series of internal processes and systems that form OoS strategic approach in managing compliance obligations.
Compliance Obligations	Compliance obligations can include legislation, regulations, industry standards and codes, charters, circulars, policies, procedures, frameworks, and codes of conduct.
Compliance Register	The Compliance Management Register is a summary list of known key compliance obligations that are applicable to the OoS. The register includes compliance responsibilities, current compliance and risk ratings, related policies and controls, and a status summary of work to improve compliance. The content is provided and maintained by all managers as appropriate. The register is stored in the Smartsheet.
Owner	The Executive Director (or other senior manager) identified as the person with overall responsibility for the compliance of that obligation.
Responsible Officer	The Owner nominated Director (or other senior manager) allocated to manage the compliance obligation and the implementation of compliance measures.

4 Roles and Responsibilities

4.1 Chief Executive

The Chief Executive is responsible for ensuring commitment to compliance is maintained; noncompliance and noncompliant behaviour are dealt with appropriately, and that a compliance function is appointed.

4.2 Executive Management

Executive management is responsible for ensuring adequate and appropriate resources are allocated to compliance management.

Responsibilities and authorities for relevant roles are to be assigned and communicated within the OoS and senior managers are to be measured against compliance outcomes.

4.3 The Audit, Risk and Governance Branch

The compliance function sits in the Audit, Risk & Governance Branch, which has authority and responsibility for the *Compliance Management Framework*. The Branch has access to:

- senior decision-makers and the opportunity to contribute early in decision-making processes,
- all levels of the organisation,
- all information and data needed to perform the compliance tasks, and
- expert advice through the Legal Services function on relevant laws, regulations, codes, and organisational standards
- provide compliance reporting to the ARC

4.4 Managers

Managers are responsible for the ongoing identification of key compliance obligations, for the evaluation and treatment of compliance risk within their span of control and for the promotion of a compliance culture.

Identified key compliance obligations are to be escalated to the appropriate level of management and recorded in the Compliance Management Register in Smartsheet.

Managers are responsible for ensuring an appropriate level of access, awareness, training and communication is provided to employees on compliance responsibilities, including relevant policies, procedures, and the Code of Conduct (within their span of control).

4.5 Compliance Owners

Compliance Owners are accountable for the ongoing identification of compliance obligations and the evaluation and treatment of compliance risk within their span of control. Identified key compliance obligations are contained in the Compliance Management Register.

Owners have overall responsibility, within their span of control, for ensuring:

- appropriate levels of awareness, training, communication, and documentation of compliance obligations is undertaken,
- responsible officers are allocated to each compliance obligation and ensure they have the appropriate capabilities to perform their compliance role,
- relevant internal and external reporting is provided,
- integration of compliance management with financial, risk, planning quality, environmental and health and safety management processes and operational procedures at the OoS,
- currency and accuracy of information contained in the Compliance Management Register and the provision of annual assurance,
- promotion of a compliance culture, and

- management and reporting of compliance breaches.

4.6 Responsible Officers

The Responsible Officer is accountable for the identification, analysis and evaluation of compliance obligations, compliance risk and the day-to-day implementation and monitoring of compliance measures.

This includes:

- providing guidance, training, and support to all employees in meeting the compliance obligation,
- liaising with appropriate internal and external parties,
- providing regular reporting on compliance risk and activity to improve compliance,
- ensuring that obligations are continually monitored, reviewed, and met throughout the OOS (including the update of the register and annual assurance activities),
- providing relevant internal and external reporting,
- promoting a compliance culture, and
- management and reporting of compliance breaches.

4.7 OoS Employees

In accordance with the Code of Conduct, it is the responsibility of all employees (commensurate with their roles, functions and span of control) to comply with relevant obligations. This includes ensuring an understanding of relevant policies and procedures.

5 Alignment with Standards

This Policy, and the *Compliance Management Framework*, remain aligned to AS/ISO 19600, pending a full review and alignment with *AS ISO 37301:2023 - Compliance management systems — Requirements with guidance for use*, due for completion by December 2023. This timeframe will also facilitate alignment with the commencement of the new *Public Interest Disclosures Act 2022*, on 13 October 2023.

Procedure

The following procedure describes the coordinated activities to:

- identify, assess, and document compliance obligations,
- ensure responsibility for meeting obligations is clearly allocated and understood,
- monitor and report assessment for how well obligations are being met, and
- manage addressing a compliance failure (or potential failure) and continually improve systems for meeting obligations.

1 Context of the Organisation

The context is to be explored to gain an understanding of the external and internal issues relevant to the purpose and strategic direction of the OoS. This will assist in determining what may affect the ability to achieve intended compliance results.

1.1 Interested Parties

The needs and expectations of interested parties (stakeholders) are to be identified, considered, and understood to improve compliance outcomes. These stakeholders are to be consulted (where appropriate), especially when updating controls and measures identified with those obligations.

This group could include government agencies (i.e. NSW Treasury), regulators, committees, and other OoS managers or subject matter experts.

1.2 Compliance Obligations

Key compliance obligations are to be identified and documented (in summary form) in the Compliance Management Register (the register). These obligations can include legislation, regulations, industry codes, standards, circulars, policies, procedures, and the Code of Conduct.

Each identified compliance obligation is to be assigned an owner and a responsible officer who must ensure the relevant compliance entry is maintained for accuracy and currency in the register.

1.2.1 Legislative Scanning

As an additional management control to assist managers in their identification of legislative compliance obligations:

- Legal Services have processes in place to monitor legislative changes, and
- Audit, Risk & Governance have processes in place to monitor the compliance landscape.

Relevant managers, who may be affected by any identified changes, are then notified to enable appropriate action. However, responsibility remains with individual managers to understand and manager relevant compliance obligations in their area.

1.3 Identification, Analysis and Evaluation of Compliance Risk

Compliance risk identification and assessment is to be undertaken using the *Enterprise Risk Management Framework*.

Obligations are to be identified and assessed so preventative controls can be developed to improve compliance with those obligations across all areas. Audit, Risk & Governance can help with this.

2 Leadership and Commitment

Leaders at all levels are to:

- apply core values and generally accepted corporate governance, ethical and community standards, and
- implement measures to promote compliant behaviour in OoS employees.

3 Planning

Strategic and business plans are to include relevant actions to:

- address compliance risks,
- promote a compliance culture, and
- achieve compliance objectives.

Where compliance with an identified obligation is assessed as less than fully compliant, action, commensurate with the level of risk, must be taken to address the compliance risk and included in appropriate plans.

4 Support

4.1 Resources

Appropriate resources are to be allocated to manage compliance risk, compliance breaches and relevant review and maintenance of relevant entries in the Compliance Management Register.

4.2 Access, Awareness, Training and Communication

An appropriate level of access, awareness, training and communication is to be provided to employees on compliance responsibilities, including relevant policies, procedures and the Code of Conduct. Each manager should ensure this is provided to their employees. Awareness can be addressed in many ways, for example, by using standing items on team meeting agendas.

Education and training of employees is to be undertaken to ensure an appropriate level of competence is maintained. This is to be assessed for effectiveness, updated as required and recorded. Each manager should ensure this is provided to their employees.

Compliance re-training is to be considered whenever there is a change of:

- role or responsibilities,
- internal processes, policies and procedures,
- organisation structure,
- compliance obligations, or
- activities, products or services.

Training should also be considered when issues arise from monitoring, auditing, reviews, complaints and non-compliance.

Managers should have ongoing communication with employees to clarify expectations and ensure the compliance message is understood. Managers should review new or changed compliance obligations, especially policies and procedures, to determine and address the impact in their area and ensure their employees understand the compliance requirements.

5 Operation

Compliance management is to be integrated with financial, risk, planning, quality, environmental, health and safety management processes and operational procedures.

Control processes are to be implemented to meet compliance obligations through defining objectives, establishing criteria, implementing controls in accordance with the criteria and documenting that the processes have been carried out as planned.

Controls are to be periodically evaluated and tested to ensure their continuing effectiveness.

Outsourced processes are to be controlled and monitored, including controlling compliance risks related to other third-party related processes (i.e. supply of goods and services).

6 Performance Evaluation

6.1 Compliance Register

The Compliance Management Register is a summary list of known key obligations under laws, regulations, codes or standards that are applicable to the OoS.

6.1.1 Links to Policies and Procedures

The register is to include information on linked internal and external policies, procedures, manuals, circulars and other documents which act as controls to improve compliance.

The 'Governance Commentary (Compliance Actions)' column provides a summary of additional activity that has been implemented to support compliance.

6.1.2 Measures to Strengthen Compliance

Measures underway to strengthen compliance are to be documented in the register in the column 'status updates of work underway'. This column can include activities such as developing or revising policies, guidelines, manuals, training, or awareness activities.

Once the measure is implemented, appropriate information in other columns is to be updated to reflect the improved control (if appropriate). The compliance rating may also benefit from a review at this point. Any change in rating would require approval by the Owner of the compliance obligation.

6.1.3 Current Compliance & Risk Rating

The register includes the current compliance rating. This is to be rated as:

- Compliant
- Compliant - controls could be strengthened
- Partially compliant
- Compliance is not assured.

The current risk rating of the compliance obligation is also to be documented.

The Audit, Risk & Governance Branch help with this assessment.

6.1.4 Update of Compliance Register

The register is to be reviewed by managers, Owners and Responsible Officers at least annually and updated where significant changes occur, or new obligations are identified.

The aim is for the register to provide sufficient evidence to show that the OoS is compliant or working towards compliance.

While each Owner and Responsible Officer is responsible for ensuring the accuracy and currency of information on the register for their area of responsibility, the register is updated with supplied information by the Audit, Risk & Governance Branch. The register is a dynamic document and is also updated on request at any time.

6.2 Quarterly Compliance Reporting

A quarterly compliance report is to be compiled by the Audit, Risk & Governance Branch from information supplied by Legal Services, Owners, Responsible Officers and other management. The report is provided to the Audit and Risk Committee (ARC) and contains information on:

- monitoring activities for the quarter,
- current compliance status (as detailed in the register),
- status of work underway to address areas where compliance is not assured,
- assurance activities, and
- new and updated legislation.

6.3 Audit

Compliance risk management is supported by audit activities and overseen by the Audit & Risk Committee (ARC).

7 Breach Management

Owners, Responsible Officers and managers are to ensure nonconformity and noncompliance events are managed. The steps include:

- identify any breaches in compliance requirements (nonconformity and noncompliance),
- promptly develop and implement an action plan for investigation and rectification of a breach or escalate to the appropriate management level for attention,
- liaise with relevant internal and external parties,
- monitor the breach rectification,
- document the breach and subsequent rectification (consider maintaining and regularly reviewing a ‘breach register’ to provide evidence of action to address breaches and to assist in identifying patterns or opportunities for improvement), and
- report to the appropriate level of management and to the ARC (if appropriate).

7.1 Assessment of Non-Compliance Issues

When noncompliance issues are identified or reported, the Owner and Responsible Officer should use the issue as an opportunity to identify any weakness in current processes that enabled the incident to occur in the first place. In addition, they should identify areas for process improvements and consider how to improve awareness of compliance obligations.

7.2 Reporting of Breaches and Actions Taken

Timely provision of information on breaches should include:

- compliance obligation breached,
- breach circumstances,
- actions being taken, and
- whether any notification to a regulator is required.

Substantial noncompliance issues are to be reported to the Owner. A compliance action plan must then be developed and tracked until the matter has been resolved. Regular reporting of these matters is to be made to the ARC and included in quarterly compliance reporting (as appropriate). The Audit, Risk & Governance Branch can help with this.

7.3 Public Interest Disclosure

All employees are encouraged to report general wrongdoing to their manager. However, for the report to be a public interest disclosure (PID) under the PID Act, it should be made to a nominated Disclosure Coordinator or Disclosure Officer (see the PID Policy and Procedure).

8 Improvement

Regular review of the framework is to incorporate feedback from employees and interested parties, including the ARC. Regular feedback can be received from Owners and Responsible Officers while undertaking annual reviews of the register and through quarterly reporting. This is to be incorporated, where appropriate, into future framework reviews.

Improvements will also be informed by the identification and treatment of nonconformity and noncompliance events (breaches), which have the potential to reduce compliance risk to the OoS and improve overall governance arrangements.