



Office  
of Sport

# **Compliance Management Policy and Procedure**

January 2016

Document information

<b>Title:</b>	Compliance Management Policy and Procedure
<b>Version:</b>	V1.0
<b>Approved date:</b>	28 January 2016
<b>Approver:</b>	Chief Executive
<b>Owner:</b>	Executive Director, Strategic and Business Services
<b>Contact:</b>	Manager Audit, Risk & Governance
<b>Publishing:</b>	This document may be published both on intranet and internet
<b>Review:</b>	Every 3 years
<b>Next Review:</b>	January 2019
<b>Related Documents and Forms:</b>	Compliance Register Compliance Reporting Template
<b>Related Policies:</b>	Compliance Management Framework Enterprise Risk Management Framework, Policy and Procedures
<b>Related External Links:</b>	Public Service Commission: The Code of Ethics and Conduct for NSW government sector employees AS3860-2006 Compliance Management Program AS/ISO19600:2015 Compliance Management Systems - Guidelines AS/NZS ISO 31000:2009 Risk Management Principles and Guidelines. TPP 15-03 Internal Audit and Risk Management Policy for the NSW Public Sector. Public Interest Disclosures Act

Document amendment history

Version	Amendments	Author	Date	Record no.
V1.0	Initial release	Manager Audit, Risk & Governance, Strategic and Business Services	28 January 2016	CDOC15/42894

# 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 this 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 Definitions

### **Compliance Management System**

The system described in the OoS Compliance Management Framework.

### **Compliance Obligations**

Compliance obligations can include legislation, regulations, industry standards and codes, charters, circulars, policies, procedures, frameworks and the *Code of Conduct*.

### **Compliance Register**

The *OoS Compliance 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.

### **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.

### **Interested Parties**

For each compliance obligation identified, there are *'interested parties'* who do not have overall responsibility for compliance with that obligation, but who have valuable input and influence into controls.

## 3 Scope

This policy applies to all OoS employees and it should be read in conjunction with the *Compliance Management Framework*.

## 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; compliance responsibilities are included in position statements of senior managers and 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 key performance measures or compliance outcomes.

### 4.3 Compliance Function

The compliance function has authority and responsibility for the compliance management framework. It has access to:

- senior decision-makers and the opportunity to contribute early in the decision-making processes;
- all levels of the organization;
- 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.

### 4.4 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.

### 4.5 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 Register*.

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).

### 4.6 Owners

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 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 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 Register* and the provision of annual assurance;
- promotion of a compliance culture; and
- management of compliance breaches.

#### **4.7 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 of compliance breaches.

# Procedure

The *Compliance Management Framework* is aligned to compliance standards and consists of elements within seven themes.

The following procedure describes the coordinated activity 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 OoS 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. 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 OoS *Compliance 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.

The register is a dynamic document that requires continual review by owners and responsible officers to ensure the accuracy and currency of content.

#### 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 across the portfolio. Relevant managers, who may be affected by any identified changes, are then notified to enable appropriate action.

### 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.

## 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

OoS strategic and business planning is to include the actions necessary 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, is to be taken to address the compliance risk and included in appropriate planning mechanisms.

### 4 Support

#### 4.1 Resources

Appropriate resources are to be allocated to manage compliance risk, compliance breaches and the maintenance of the *Compliance Register*.

#### 4.2 Access, Awareness, Training and Communication

An appropriate level of access, awareness, training and communication is to be provided to OoS employees on compliance responsibilities, including relevant policies, procedures and the *Code of Conduct*.

Awareness can be addressed in a number of ways, for example, through the use of 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.

Compliance retraining is to be considered whenever there is a change of:

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

It is to also be considered when issues arise from monitoring, auditing, reviews, complaints and non-compliance.

Communication is to be on-going to clarify OoS expectations of employees and to ensure the compliance message is understood by all employees.

### 5 Operation

Compliance management is to be integrated with financial, risk, planning, quality, environmental, health and safety management processes and operational procedures at the Office of Sport (OoS).

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 *OoS Compliance 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 control methods.

The latest publishing date of internal documents is also to be included.

If work is underway to revise or implement OoS policies and procedures, this is to be summarised in the column *'status updates of work underway...'*. Governance Commentary (Compliance Actions)

This column in the register provides a summary of additional activity that has been implemented to support compliance.

Where an external annual attestation or reporting is also required, the day and month is to be included.

#### 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'*. The entry is to include the date and the title of the information provider (i.e. *'Oct-15 D.P&C: Revision of the Gifts & Benefits policy is currently out for consultation'*).

This column can include activities such as developing or revising policies, guidelines, manuals, training, workshops 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; or
- Compliance is not assured.

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

#### 6.1.4 Update of Compliance Register

The register is to be reviewed 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 currency of information on the register for their area of responsibility, the register is updated with supplied information by the Audit, Risk & Governance function.

The register is a dynamic document and is also updated upon request at any time.



## 6.2 Quarterly Compliance Reporting

A quarterly compliance report is to be compiled by Audit, Risk & Governance from information supplied by Legal Services, owners and responsible officers. 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)
- Current status of work underway to address areas where compliance is not assured;
- Assurance activities; and
- New and updated policies.

## 6.3 Audit

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

### 6.3.1 Annual Updates and Assurance

The assurance process includes annual formal management review of the *Compliance Register*, completion of an *Annual Compliance Declaration* by Executive Directors and provision of the register to the ARC for endorsement.

The Audit, Risk & Governance function will communicate with responsible officers and owners to ensure the register contains accurate and current information. Once confirmation is received or information updated, the approved register is to be submitted to the ARC for endorsement.

The month and year of the most recent review is to be recorded in the register.

## 7 Improvement

Regular review of the framework is to incorporate feedback from employees and interested parties, including the ARC.

Improvements will also be informed by the identification and treatment of nonconformity and noncompliance events, which has the potential to reduce compliance risk to the OOS and improve overall governance arrangements.

### 7.1 Compliance Framework

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.

### 7.2 Breach Management

As part of the ongoing improvement process, compliance breaches are to be managed. The steps to be taken include:

- Identify and report any breaches in compliance requirements (nonconformity and noncompliance);
- Promptly develop and implement an action plan for investigation and rectification of a breach;
- Liaise with relevant internal and external parties;
- Monitor the breach rectification; and
- Document the breach and subsequent rectification.

#### 7.2.1 Assessment of Non-Compliance Issues

When non-compliance issues are 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, and also those areas in which to make process improvements or improve awareness of compliance obligations.

### **7.2.2 Reporting of Breaches and Actions Taken**

A basic element of compliance reporting is the provision of timely information on any breaches that have occurred, including:

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

Substantial non-compliance 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 Audit & Risk Committee as well as a status update within quarterly compliance reporting (as appropriate).

### **7.2.3 Public Interest Disclosure**

Non-compliance issues of a confidential or sensitive nature can be reported directly to the Director, People & Culture, who will then ensure management of the disclosure in accordance with the *Public Interest Disclosures Act*.