

august09



New South Wales  
TREASURY

tpp  
09-05

**Internal Audit and Risk Management Policy  
for the NSW Public Sector**

---

OFFICE OF FINANCIAL MANAGEMENT  
**Policy & Guidelines Paper**

## Preface

Corporate governance - which refers broadly to the processes by which organisations are directed, controlled and held to account - matters. Effective corporate governance arrangements are *essential* to the performance, integrity and transparency of public sector organisations.

In March 2008, following a comprehensive review of internal audit capacity in the NSW public sector, the Government approved an integrated suite of corporate governance practices to strengthen the 'whole of government' policy and regulatory arrangements for internal audit and risk management.

Treasury Circular NSW TC 09/08 implements the new "Internal Audit and Risk Management Policy" which draws on the practice of exemplar organisations in the public and private sectors. This Policy & Guidelines Paper sets out the requirements of the new policy.

The policy is issued as a direction to department heads and statutory bodies, and it withdraws and replaces NSW Treasury Policy & Guidelines Papers TPP 95a, TPP 95b and TPP 97-3.

This policy is not a requirement for State Owned Corporations which should refer to Treasury's Commercial Policy Framework for corporate governance guidelines.

The policy aims to ensure that NSW departments and statutory bodies maintain organisational arrangements that provide additional assurance, independent from operational management, on internal audit and risk management.

To achieve this, the policy mandates a set of 'core requirements' that departments and statutory bodies must implement for consistent application across the sector.

The core requirements comprise key governance practices that ensure the real and perceived independence of the Audit and Risk Committee, the Chief Audit Executive and the Internal Audit function, as well as the adoption of current standards for professional practice in internal audit and risk management.

Consistent with better practice corporate governance principles, the new policy requires department heads and governing boards of statutory bodies to attest compliance with the core requirements annually, and to provide this information in a new annual report disclosure.

This Policy & Guidelines Paper provides departments and statutory bodies with the procedures they need to implement the core requirements of the policy.

**Michael Schur**  
**Secretary**  
NSW Treasury  
August 2009

**Treasury Ref:** TPP09-5  
**ISBN:** 978-0-7313-3424-7

---

### Note

General inquiries concerning this document should be initially directed to:  
Dr Michael Di Francesco (Tel: 9228 3951, or E-mail:  
[michael.difrancesco@treasury.nsw.gov.au](mailto:michael.difrancesco@treasury.nsw.gov.au)) of NSW Treasury.

This publication can be accessed from the Treasury's Office of Financial Management Internet site [<http://www.treasury.nsw.gov.au/>].  
For printed copies contact the Publications Officer on Tel: 9228 4426.

---

## Contents

	<u>Page</u>
Preface	i
Executive Summary	1
Acknowledgements	2
Part A: The Internal Audit and Risk Management Policy	3
Part B: Instructions for Implementing the Core Requirements	10
Core Requirement 1. Internal Audit Function	10
Core Requirement 2. Audit and Risk Committee	16
Core Requirement 3. Independent Chairs and Members	17
Core Requirement 4. Model Charter and Committee Operations	21
Core Requirement 5. Risk Management Standards	26
Core Requirement 6. Internal Audit Standards	32
Annexe A: Better Practice Framework for Internal Audit	37
Annexe B: Model Internal Audit Charter	38
Annexe C: Model Audit and Risk Committee Charter	43
Annexe D: Attestation Statement Template (Internal Audit and Risk Management Policy Compliance)	50
Annexe E: Internal Audit and Risk Management Statement Template (Annual Report Disclosure)	54

## Executive Summary

NSW Treasury Circular NSW TC 09/08 implements the *Internal Audit and Risk Management Policy for the NSW Public Sector* (the Policy). The Policy requires department heads and governing boards of statutory bodies to attest and report compliance with a prescribed set of 'core requirements' annually.

The Policy, including the procedures that department heads and governing boards of statutory bodies must follow to be compliant with the 'core requirements', is set out in this Policy & Guidelines Paper. The six core requirements comprise:

- § Core Requirement 1: Internal Audit Function - this covers the requirement to establish and maintain an Internal Audit function
- § Core Requirement 2: Audit and Risk Committee - this covers the requirement to establish and maintain an Audit and Risk Committee
- § Core Requirement 3: Independent Chairs and Members - this covers Committee composition, and the requirement to appoint an independent chair and a majority of independent members
- § Core Requirement 4: Model Charter and Committee Operations - this covers the requirements to maintain governance arrangements that ensure both the real and perceived independence of the Committee and the rigour and quality of its oversight and monitoring role
- § Core Requirement 5: Risk Management Standards - this covers the requirement to implement a risk management process that is appropriate to the needs of the department or statutory body and consistent with the current risk standard, i.e. AS/NZS 4360: 2004 *Risk Management*
- § Core Requirement 6: Internal Audit Standards - this covers the requirement to ensure that operation of the Internal Audit function is consistent with the relevant standard, i.e. IIA *International Standards for the Professional Practice of Internal Auditing* and any additional practice requirements set by the Policy.

To comply with the Policy, the department head or governing board of the statutory body must review existing arrangements for internal audit and risk management against the 'core requirements', and take steps to either establish relevant governance structures where these do not exist or align existing governance structures with the new requirements.

The department head or governing board of the statutory body is required annually to:

- § attest compliance with the core requirements for the prior financial year (the 'reporting period') annually - the department head or governing board of the statutory body must use the relevant Attestation Statement Template at [Annexe D](#) of this Policy & Guidelines Paper
- § report compliance with the core requirements for the prior financial year (the 'reporting period') in the Annual Report relating to that period - the department head or governing board of the statutory body must use the relevant Internal Audit and Risk Management Statement Template at [Annexe E](#) of this Policy & Guidelines Paper.

For a limited number of departments and statutory bodies compliance with the core requirements may not be achievable by the implementation deadline. Where this is the case, an exception to the core requirement(s) must be determined by the Portfolio Minister. The department head or governing board of the statutory body may seek an exception from the core requirement(s) by making a written request to the Portfolio Minister for a determination.

## Acknowledgements

In preparing this Policy & Guidelines Paper NSW Treasury has drawn on the standards developed and endorsed by professional associations and the policy and practice of exemplar public sector organisations across Australia.

Key elements of the procedures in this Policy & Guidelines Paper reflect a range of 'better practices' extracted from guidelines developed in comparable public sector organisations, and modified and adapted for the NSW public sector context.

NSW Treasury wishes to acknowledge that the following policy documents and standards have been consulted in the preparation of this Policy & Guidelines Paper:

Australian Capital Territory (ACT) Department of the Treasury for:

§ [Internal Audit Framework, April 2007.](#)

Institute of Internal Auditors (IIA) for:

§ [International Standards for the Professional Practice of Internal Auditing, January 2009.](#)

Standards Australia / Standards New Zealand for:

§ [AS/NZS 4360: 2004 Risk Management, 2004.](#)

Victoria Department of Treasury and Finance for:

§ [Standing Directions of the Minister for Finance and Associated Rules and Supplementary Material, July 2008.](#)

In particular, NSW Treasury acknowledges that material has been reproduced from the following better practice guidelines, all of which are copyright of the Commonwealth of Australia and reproduced by permission:

Australian National Audit Office (ANAO) for:

§ [Public Sector Internal Audit: An Investment in Assurance and Business Improvement, Better Practice Guide, September 2007.](#)

§ [Public Sector Audit Committees, Better Practice Guide, February 2005.](#)

Comcover for:

§ [Risk Management, Better Practice Guide, June 2008.](#)

## Part A: Internal Audit and Risk Management Policy

### Background

In 2007, the Department of Premier and Cabinet (DPC) completed a performance review of internal audit capacity in the NSW public sector.

The review's key recommendation was to strengthen the 'whole of government' policy and regulatory framework for the governance of internal audit and risk management.

The review outlined a 'better practice' approach to internal audit and risk management that draws on the standards endorsed by professional associations and the practice of exemplar organisations in the public and private sectors. A summary of this 'better practice' approach, extracted from the review, appears at [Annexe A](#) to this Policy & Guidelines Paper.

The Government has approved the review's recommendations, and the final report [Internal Audit Capacity in the NSW Public Sector](#) issued in April 2008.

The *Internal Audit and Risk Management Policy for the NSW Public Sector* ('the Policy') is set out in this Policy & Guidelines Paper.

The Policy implements approved actions of the April 2008 DPC performance review and must be read in conjunction with DPC Circular C2009-13 *Prequalification Scheme: Audit and Risk Committees*.

### Purpose of the Policy

The corporate governance practices required by the Policy aim to strengthen internal audit, risk management and governance processes across the NSW public sector, and promote the integrity of, and accountability for, the allocation and management of the State's resources.

The purpose of the Policy is to ensure that department heads and governing boards of statutory bodies establish and maintain organisational arrangements that will provide additional assurance, independent from operational management, on internal audit and risk management. The Policy does this by:

- § introducing corporate governance requirements to ensure the real and perceived independence of the Audit and Risk Committee, the Chief Audit Executive and Internal Audit function and
- § adopting the application of current standards for professional practice in internal audit (the Institute of Internal Auditors (IIA) *International Standards for the Professional Practice of Internal Auditing* available at [www.theiia.org](http://www.theiia.org)) and risk management (Australian Standard AS/NZS 4360: 2004 *Risk Management* available at [www.riskmanagement.com.au](http://www.riskmanagement.com.au)) except where these standards are in conflict with the Policy or any related guidelines issued by NSW Treasury.<sup>1</sup>

---

<sup>1</sup> At the time of writing, the International Organisation for Standardization (ISO) was finalising a new international standard on risk management, ISO 31000 *Risk Management - Principles and guidelines on implementation*. ISO 31000 is expected to consolidate existing AS/NZS 4360: 2004 guidance on the risk management process by recommending its implementation as part of an organisation's 'risk management framework'. However, ISO 31000 is also expected to introduce additional requirements. Standards Australia is currently considering a proposal to adopt ISO 31000.

The Policy requires department heads and governing boards of statutory bodies to attest compliance with the six 'core requirements' specified in Part B of this Policy & Guidelines Paper annually, and to report this attestation within the annual report of the respective department or statutory body.

Department heads and governing boards of statutory bodies should refer to the Policy when reviewing and implementing their organisational arrangements for internal audit and risk management. Departments and statutory bodies are also encouraged to refer to the relevant professional standards and guidelines referenced in the Policy for more information.

## Application of the Policy

### Departments and Statutory Bodies

Treasury Circular NSW TC 09/08 issues this policy as a Direction to:

- § 'department heads' under section 18 of the [Annual Reports \(Departments\) Act 1985](#)
- § 'statutory bodies' under section 15 of the [Annual Reports \(Statutory Bodies\) Act 1984](#)
- § 'officers of an authority' and 'accounting officers' under section 9 of the [Public Finance and Audit Act 1983](#).

For the purposes of the Policy, a department head means a 'department head' as defined in section 3 of the *Annual Reports (Departments) Act 1985*, and a statutory body means a 'statutory body' as defined in section 3 of the *Annual Reports (Statutory Bodies) Act 1984*.

The Policy requires an 'officer of an authority' and 'accounting officer' (defined in section 4 of the *Public Finance and Audit Act 1983*) to do all that is necessary to ensure that the department head or governing board of the statutory body is able to comply with the attestation requirements.

**The implementation date for departments and statutory bodies to comply with the 'core requirements' is the end of the financial year ending on or after 30 June 2010.**

### State Owned Corporations

For statutory State Owned Corporations, section 20L of the [State Owned Corporations Act 1989](#) charges the board of directors with governance of the entity.

Under Treasury's Commercial Policy Framework, Treasury issues State Owned Corporations (SOCs) with corporate governance guidelines which mirror standards that are recommended for Australian Securities Exchange listed companies.

Statutory SOC's should, therefore, maintain arrangements for internal audit and risk management that are consistent with these standards and, where appropriate, apply any additional requirements set out in the Policy.

## Relationship to legislation and existing policies

### Public Finance and Audit Act 1983 requirements

The Policy does not alter the [Public Finance and Audit Act 1983](#) section 11(2) requirement that, wherever practicable, the Head of an Authority shall establish and maintain an effective internal audit organisation.

The Policy sets out how department heads and governing boards of statutory bodies should comply with this legal requirement for internal audit.

### Existing Treasury internal audit and risk management policies

The Policy withdraws and replaces the following NSW Treasury Policy and Guidelines Papers:

- § TPP 95a *Statement of Best Practice – Internal Control and Internal Audit*
- § TPP 95b *Internal Control Assessment*
- § TPP 97-3 *Risk Management and Internal Control Toolkit*

### Related internal audit policies

The Policy must be read in conjunction with related audit and risk policies issued by the Department of Premier and Cabinet, including:

- § [NSW Treasury and Department of Commerce - Prequalification Scheme: Audit and Risk Committee Independent Chairs and Members Scheme Conditions January 2009](#)
- § [Department of Premier and Cabinet Circular No. 2009-13 - Prequalification Scheme: Audit and Risk Committees May 2009](#)
- § [Department of Premier and Cabinet and Department of Commerce - Prequalification Scheme: Audit and Risk Committee Independent Chairs and Members Guidelines for Agencies and Members May 2009.](#)

## Core Requirements of the Policy

Department and statutory body compliance with the Policy will be monitored for the 'core requirements' that need immediate implementation and consistent application across the sector.

The core requirements will strengthen the governance arrangements for internal audit and risk management by mandating compliance to a level that is consistent with benchmarked 'better practice'.

The 'core requirements' are set out in Part B of this Policy & Guidelines Paper and comprise:

- § Core Requirement 1: Internal Audit Function - this covers the requirement to establish and maintain an Internal Audit function
- § Core Requirement 2: Audit and Risk Committee - this covers the requirement to establish and maintain an Audit and Risk Committee
- § Core Requirement 3: Independent Chairs and Members - this covers Committee composition, and the requirement to appoint an independent chair and a majority of independent members
- § Core Requirement 4: Model Charter and Committee Operations - this covers the requirements to maintain governance arrangements that ensure both the real and perceived independence of the Committee and the rigour and quality of its oversight and monitoring role

- § Core Requirement 5: Risk Management Standards - this covers the requirement to implement a risk management process that is appropriate to the needs of the department or statutory body and consistent with the current risk standard, i.e. AS/NZS 4360: 2004 *Risk Management*
- § Core Requirement 6: Internal Audit Standards - this covers the requirement to ensure that operation of the Internal Audit function is consistent with the relevant standard, i.e. IIA *International Standards for the Professional Practice of Internal Auditing* and any additional practice requirements set by the Policy.

To comply with the Policy, the department head or governing board of the statutory body must review existing arrangements for internal audit and risk management against the 'core requirements', and take steps to either establish relevant governance structures where these do not exist or align existing governance structures with the new requirements.

The department head or governing board of the statutory body is required to attest compliance with the core requirements annually.

The department head or governing board of the statutory body must report compliance with the core requirements for the prior financial year ('the reporting period'):

- § to the Treasurer no later than two months after year end by using the Attestation Statement Template, and
- § in the Annual Report by way of a short disclosure using the Internal Audit and Risk Management Statement Template.

#### Requirements for Attestation

The department head or governing board of the statutory body is required to attest compliance with the core requirements for the prior financial year (the 'reporting period') annually.

The department head or governing board of the statutory body must use the relevant Attestation Statement Template at [Annexe D](#) of this Policy & Guidelines Paper.

The department head or governing board of the statutory body must submit the first attestation statement for the financial year ending on or after 30 June 2010 to the Treasury (on behalf of the Treasurer) no later than two (2) months after year end. Submissions should be addressed to:

The Senior Director  
Financial Management and Reporting Branch  
NSW Treasury  
Level 24, Governor Macquarie Tower  
1 Farrer Place  
Sydney NSW 2000.

The purpose of this initial attestation statement is to attest that the department or statutory body has the core requirements in place by the end of the financial year ending on or after 30 June 2010, unless otherwise determined by the Portfolio Minister.

For subsequent reporting periods (commencing with the financial year ending on or after 30 June 2011) the purpose of the attestation statement is to attest that the department or statutory body has the core requirements in operation for the relevant reporting period, unless otherwise determined by the Portfolio Minister.

## Requirements for Annual Reporting Disclosures

The department head or governing board of the statutory body is required annually to report compliance with the core requirements for the prior financial year (the 'reporting period') in the Annual Report relating to that period.

The department head or governing board of the statutory body must use the relevant Internal Audit and Risk Management Statement Template at [Annexe E](#) of this Policy and Guidelines Paper.

In terms of presentation within the Annual Report, the department head or governing board of the statutory body must ensure that the Internal Audit and Risk Management Statement is co-located in the Annual Report with the existing requirement to disclose 'risk management and insurance activities'.

## Exceptions Process

For a limited number of departments and statutory bodies compliance with the core requirements of the Policy may not be achievable by the implementation deadline.

Where this is the case, a department head or governing board of the statutory body may apply for an exception from the core requirement(s) provided the department head or governing board of the statutory body satisfactorily demonstrates that:

- § the department or statutory body cannot comply because resourcing constraints will materially impact the department's or statutory body's operating budget (in which case, the department head or governing board of the statutory body must first determine whether central agency cluster initiatives are available to them prior to seeking an exception on this basis) and/or
- § current or proposed alternative arrangements will achieve outcomes equivalent to the requirement(s) (in which case, any proposed alternative arrangements must be implemented no later than the end of the financial year ending on or after 30 June 2011).

An exception to the core requirement(s) must be determined by the Portfolio Minister.

The department head or governing board of the statutory body may seek an exception from the core requirement(s) by making a written request to the Portfolio Minister for a determination. The written request must either:

- § provide reasons why the department or statutory body cannot comply with the requirement(s) or
- § describe and demonstrate the department's or statutory body's efforts to implement alternative arrangements and how these will achieve an outcome equivalent to the requirement(s) or
- § describe why efforts to access alternative arrangements have not been successful.

For the initial reporting period (i.e. the financial year ending on or after 30 June 2010) the department head or governing board of the statutory body must seek an exception to the core requirement(s), and gain a determination by the Portfolio Minister, prior to the end of the third quarter of the reporting period to which the exception will apply (e.g. 31 March 2010 for the financial year ending on 30 June 2010).

For subsequent reporting periods (i.e. commencing with the financial year ending on or after 30 June 2011), the department head or governing board of

the statutory body must seek an exception to the core requirement(s), and gain a determination by the Portfolio Minister, prior to the end of the second quarter of the reporting period to which the exception will apply (e.g. 31 December 2010 for the financial year ending on 30 June 2011).

A determination in respect of the exceptions criteria will be operative for the one reporting period only and, even where the circumstances for the initial exception are ongoing, must be renewed annually.

The department head or governing board of the statutory body is required to indicate on the Attestation Statement (refer [Annexe D](#) of this Policy & Guidelines Paper) where an exception from a core requirement has been determined by the Portfolio Minister.

In such cases, the department head or governing board of the statutory body must retain documentary evidence of the Portfolio Minister's determination, and submit this material to Treasury (on behalf of the Treasurer) as an attachment to the Attestation Statement no later than two months after year end.

## Support for implementing the Policy

The Government has implemented initiatives to assist department heads and statutory bodies to comply with the Policy's core requirements. These initiatives include:

- § establishing a pre-qualification panel scheme for independent chairs and members of Audit and Risk Committees (DPC Circular C2009-13 *Prequalification Scheme: Audit and Risk Committees*)
- § facilitating an audit and risk management network for public sector practitioners (the NSW Public Sector Audit and Risk Practitioner Network) and
- § promulgating an internal audit human resource strategy.

Department heads and statutory bodies may consider other strategies to achieve the Policy's core requirements such as establishing, through central agency coordination, a cluster-based, sharing arrangement for internal audit governance and resourcing.

Further information on these initiatives will be made available on a dedicated section of the NSW Treasury website: [www.treasury.nsw.gov.au](http://www.treasury.nsw.gov.au)

## Monitoring of Policy compliance

The Policy requires that department heads and statutory bodies provide a brief Internal Audit and Risk Management Statement disclosure in the Annual Report indicating the department head or governing board of the statutory body has completed and submitted an Attestation Statement to the Treasury (on behalf of the Treasurer) and is compliant with the core requirements.

The Auditor-General may undertake an assurance role in monitoring the sector's compliance with the core requirements outlined in the Policy. Each year, the Auditor-General may conduct a review of department and statutory body compliance with the Policy by conducting a compliance engagement on a sample of departments and statutory bodies.

NSW Treasury will, on a periodic basis, review the operation of the Policy to assess the efficiency and effectiveness of the arrangements, as well as to assess the sector's compliance with the core requirements outlined in the Policy.

### Explanatory note for reading the Policy: Statutory Bodies

For statutory bodies, the establishing legislation is the primary source of information on the board's role, functions and reporting arrangements. There are, however, principally two types of boards: governing and advisory.

**Governing** boards are responsible for the governance of the entity, including leading and controlling the organisation and monitoring executive management.

**Advisory** boards are established to provide advice to the Minister on matters relevant to the management of the entity, and are subject to control and direction by the Minister.

In this Policy, the term '**governing board of the statutory body**' means the **body of persons who are responsible for the governance of the entity**, and therefore accountable for attesting to and ensuring compliance with the Policy. This will apply to most statutory bodies.

For those statutory bodies with an advisory board or, in a small number of cases no governing board, the chief executive officer (or person who exercises the functions of chief executive officer in relation to the statutory body) is the person responsible for the governance of the entity. **In these cases, the chief executive officer (or person who exercises the functions of chief executive officer in relation to the statutory body) is responsible for ensuring compliance with the requirements set out in the Policy.**

For more information on the roles of boards refer to [Department of Premier and Cabinet, \*An Introduction to Board and Committee Membership\*, July 2002](#) and [Audit Office of New South Wales, \*On Board: Guide to Better Practice for Public Sector Governing and Advisory Boards\*, April 1998](#).

## Part B: Instructions for Implementing the Core Requirements

### Core Requirement 1

**An Internal Audit function has been established and maintained.**

#### 1.1 Definition of Internal Audit

##### 1.1.1

This Policy adopts the Institute of Internal Auditors (IIA) definition of 'internal audit' as 'an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes'.

##### 1.1.2

The IIA definition covers two types of internal audit services:

- § 'assurance services' – an objective examination of evidence for the purpose of providing an independent assessment of risk management, control or governance processes for the organisation, and
- § 'consulting services' – advisory and related client activities, the nature and scope of which are agreed upon with the client and which are intended to add value and improve an organisation's operations.

In this Policy, internal audit services may include either or both of these service categories.

#### 1.2 The Internal Audit Function

##### 1.2.1

The department head or governing board of the statutory body must ensure there is an operational and adequately resourced Internal Audit function.

##### 1.2.2

In this Policy, an 'Internal Audit function' means either an 'in-house' internal audit service delivery model or an 'out-sourced' internal audit service delivery model. The department head or governing board of the statutory body must:

- § determine the appropriate service delivery model for the Internal Audit function based on the department's or statutory body's needs, which may change over time as circumstances change, and
- § ensure that the service delivery model selected will provide assurance, independent from operational management, on risk management, control and governance processes.

The range of service delivery models is described in Sections 1.2.3 and 1.2.4 of this Policy.

##### 1.2.3

Where the department head or governing board of the statutory body establishes the Internal Audit function using an in-house service delivery model, the function is defined as being exclusively or predominantly provided and managed by a department's or statutory body's resources.

## 1.2.4

Where the department head or governing board of the statutory body establishes the Internal Audit function using an out-sourced service delivery model, the function is defined as being one or other of the following:

- § co-sourced service delivery with in-house management, where the department or statutory body provides and manages internal audit services through a combination of in-house resources and contracted services delivered by an appropriately qualified third party provider
- § out-sourced service delivery with in-house management, where the department or statutory body provides and manages internal audit services through contracted services delivered by an appropriately qualified third party provider
- § out-sourced service delivery, where the department or statutory body provides all internal audit services through contracted services delivered by an appropriately qualified third party provider and only the contracted services are project managed in-house.

## 1.2.5

Where the Internal Audit function is established using an out-sourced service delivery model (as defined in Section 1.2.4), the department head or governing board of the statutory body must ensure that an experienced senior employee of the department or statutory body is appointed as the in-house liaison officer and/or contract manager for any internal audit services delivered by a third party provider. This is to ensure that the department or statutory body retains control of the internal audit strategic direction and is able to actively monitor the performance of the third party provider.

## 1.2.6

When determining the most appropriate service delivery model for the Internal Audit function, the department head or governing board of the statutory body must give due regard to the following factors:

- § the size of the department or statutory body, in terms of both staffing levels and budget
- § the complexity of the department's or statutory body's core business
- § the risk profile of the department's or statutory body's operations
- § the geographical and functional distribution of the department's or statutory body's operations
- § the viability of alternative service delivery models and the ability of the department or statutory body to attract and retain suitable staff, including professional staff for in-house service delivery, and experienced contract managers for out-sourced service delivery
- § the overall cost of alternative service delivery models, including the salaries and overheads of in-house professional staff, and the costs of contract management and delivery for out-sourced service delivery
- § the capacity of alternative service delivery models to deliver flexibility in the internal audit work-plan.

## 1.2.7

As defined in Section 1.2.4, an out-sourced service delivery model for the Internal Audit function may include utilisation by the department head or governing board of the statutory body of pooled Internal Audit resources made available through a shared service or policy cluster arrangement facilitated by the Department of Premier and Cabinet under the Policy.

#### 1.2.8

The department head or governing board of the statutory body is required to set out which service delivery model for the Internal Audit function has been established in the department or statutory body, including the reasons for establishing that model, in the annual Attestation Statement required by the Policy.

### 1.3 The Chief Audit Executive

#### 1.3.1

The department head or governing board of the statutory body must appoint a Chief Audit Executive to head the Internal Audit function. The Chief Audit Executive is the most senior position within the department or statutory body with responsibility for internal audit and the position holder must:

- § be classified at a sufficiently senior level to ensure that the position holder is able to discuss and negotiate internal audit results with senior management on a reasonably equal footing
- § possess skills, knowledge and personal qualities that can ensure the credibility and acceptance of the Internal Audit function they lead.

#### 1.3.2

The Chief Audit Executive reports to the department head or governing board of the statutory body. However, the department head or governing board of the statutory body must ensure the operational independence of the Internal Audit function by establishing 'dual reporting lines' for the Chief Audit Executive. The requirements for dual reporting lines are set out in Sections 1.5 and 4.3 of this Policy.

#### 1.3.3

Where the Internal Audit function is established using an out-sourced service delivery model, the Chief Audit Executive is the most senior position within a department or statutory body with responsibility for internal audit.

#### 1.3.4

The department head or governing board of the statutory body must consult with the Audit and Risk Committee when designating, appointing or removing a Chief Audit Executive. Consultation will include either seeking the advice of the Chair of the Audit and Risk Committee, or involving an independent member of the Audit and Risk Committee in the selection process. The Audit and Risk Committee is discussed in Section 2.1 of this Policy.

## 1.4 Charter for the Internal Audit Function

### 1.4.1

The department head or governing board of the statutory body must ensure that the Internal Audit function has a Charter that is consistent with the content of the 'model charter' at [Annexe B](#) of this Policy. The model charter sets out 'common' content for an Internal Audit Charter and covers the following structural elements:

- § purpose of internal audit
- § independence
- § authority and confidentiality
- § roles and responsibilities
- § scope of internal audit activity
- § standards
- § relationship with external audit
- § planning and reporting
- § administrative arrangements
- § review of charter.

### 1.4.2

The Internal Audit Charter must be developed by the Chief Audit Executive and approved by the department head or governing board of the statutory body on the advice of the Audit and Risk Committee.

### 1.4.3

The department head or governing board of the statutory body is required to consider the specific circumstances of the department or statutory body and may, where appropriate, and on advice from the Audit and Risk Committee, include provisions additional to those set out in the model charter, providing these do not conflict with the model charter.

## 1.5 Governance of the Internal Audit Function

### 1.5.1

The department head or governing board of the statutory body must ensure there is a clear separation of operational management from the Internal Audit function.

### 1.5.2

To achieve operational independence of the Internal Audit function, the department head or governing board of the statutory body must ensure that the Chief Audit Executive has a dual reporting line. A dual reporting line means that the Chief Audit Executive must:

- § report administratively to the department head or governing board of the statutory body to facilitate day-to-day operations of the Internal Audit function,<sup>1</sup> and
- § report functionally to the Audit and Risk Committee for strategic direction and accountability of the Internal Audit function.

---

<sup>1</sup> In the case of a statutory body, it may be appropriate for the Chief Audit Executive to report administratively to either the chief executive of the statutory body or a delegate director of the board.

### 1.5.3

The department head or governing board of the statutory body must ensure that Internal Audit reporting lines are clearly documented within the Internal Audit Charter. Section 4.3 of this Policy also requires documentation of the dual reporting line structure in the Audit and Risk Committee Charter.

### 1.5.4

The Audit and Risk Committee oversees the Internal Audit function by reviewing and approving Internal Audit plans.

### 1.5.5

The department head or governing board of the statutory body must ensure that the Internal Audit function is appropriately positioned within the department's or statutory body's governance framework to work with external audit and internal business units.

### 1.5.6

The department head or governing board of the statutory body must ensure the Internal Audit function is operationally independent from the activities it audits.

## 1.6 Resourcing of the Internal Audit Function

### 1.6.1

The department head or governing board of the statutory body must ensure that the Internal Audit function has a budget, and access to sufficient professional staff resources with the necessary skills and experience, that are sufficient relative to the risks facing the department or statutory body.

### 1.6.2

The department head or governing board of the statutory body must determine the budget and level of resourcing on advice from the Audit and Risk Committee. Where the Audit and Risk Committee considers that the level of resourcing for the Internal Audit function is insufficient relative to the risks facing the department or statutory body, it should draw this to the attention of the department head or governing board of the statutory body. The Chair of the Audit and Risk Committee must ensure that the Committee's review of, and recommendations on, proposed allocations of resources are minuted by the Committee's secretariat.

### 1.6.3

The department head or governing board of the statutory body must ensure that professional staff of the Internal Audit function have reasonable access to training and professional development through the relevant professional associations, e.g. Institute of Internal Auditors (IIA), Certified Practising Accountants (CPA) etc.

### 1.6.4

The department head or governing board of the statutory body must ensure that all professional staff are provided with sufficient and up-to-date information on the entity's risks and operations in order for them to perform their roles and discharge their responsibilities.

## 1.7 Internal Audit Quality Assurance and Improvement

### 1.7.1

Where the Internal Audit function is established using an in-house service delivery model (as defined in Section 1.2.3 of this Policy), the department head or governing board of the statutory body must ensure there is a documented and operational Quality Assurance and Improvement Program for the Internal Audit function. Where the Internal Audit function is established using an outsourced service delivery model (as defined in Section 1.2.4 of this Policy), the third party provider of internal audit services must operate an equivalent quality assurance program.

### 1.7.2

The department head or governing board of the statutory body must ensure that the Internal Audit function, whether in-house or outsourced, satisfies assessment against the relevant professional standards, i.e. IIA annual internal assessment and external assessment at least every five (5) years.

### Useful reference documents

- § [Australian National Audit Office \(ANAO\) \*Public Sector Internal Audit: An Investment in Assurance and Business Improvement, Better Practice Guide \(2007\)\*](#)
- § [Department of Premier and Cabinet \(DPC\) \*Performance Review: Internal Audit Capacity in the NSW Public Sector \(2008\)\*](#)
- § [Institute of Internal Auditors \(IIA\) \*International Standards for the Professional Practice of Internal Auditing \(2009\)\*](#)
- § [Institute of Internal Auditors \(IIA\) \*Frequently Asked Questions\*](#)
- § [Institute of Internal Auditors \(IIA\) \*Structured Programs and Courses\*](#)
- § [Institute of Internal Auditors \(IIA\) \*Audit Committee Briefings, Internal Audit Standards: Why They Matter \(2005\)\*](#)

## Core Requirement 2

### An Audit and Risk Committee has been established.

#### 2.1 The Audit and Risk Committee

##### 2.1.1

The department head or governing board of the statutory body must establish an Audit and Risk Committee to oversee and monitor governance, risk and control issues affecting the operations of the department or statutory body.

##### 2.1.2

The establishment, composition and governance of the Audit and Risk Committee must be in accordance with this Policy. The Audit and Risk Committee is an integral component of a department's or statutory body's corporate governance arrangements, and its responsibilities will generally cover review and oversight of the following areas:

- § internal controls
- § risk management
- § corruption and fraud prevention
- § external accountability (including the financial statements)
- § applicable laws and regulations
- § internal audit
- § external audit.

Directions relating to the roles and responsibilities of an Audit and Risk Committee are contained in Sections 4.1 - 4.5 of this Policy.

##### 2.1.3

There may be circumstances where the department head or governing board of the statutory body has established separate oversight committees: an Audit Committee and a Risk Committee. Where, prior to the issue of this Policy, a department or statutory body is operating a Risk Committee separate to the Audit Committee, the department head or governing board of the statutory body must transfer the 'risk management' oversight responsibilities of the existing Risk Committee to the Audit Committee, and establish an 'Audit and Risk Committee'. The 'risk management' oversight responsibilities are defined in Section 5.8 of this Policy, and also set out in the 'risk management' section of the Model Audit and Risk Committee Charter (at [Annexe C](#) of this Policy).

##### 2.1.4

Where an Audit and Risk Committee has been reconstituted as provided for in Section 2.1.3 of this Policy, the department head or governing board of the statutory body must ensure that the roles and responsibilities, composition and governance of the Committee is in accordance with the Policy.

### Core Requirement 3

The Audit and Risk Committee has an independent chair and a majority of independent members. The Audit and Risk Committee has at least three members, and no more than five members.

#### 3.1 Membership of the Committee

##### 3.1.1

The term 'independent member' (including 'independent chair') is defined in Section 3.3 of this Policy. In complying with this core requirement, the department head or governing board of the statutory body must adhere to the independence requirements set out in Section 3.3.

##### 3.1.2

The Chair of the Audit and Risk Committee must be independent.

##### 3.1.3

The Chair is counted as one member of the Audit and Risk Committee.

##### 3.1.4

The Audit and Risk Committee must have no fewer than three (3) members, and no more than five (5) members, of whom a majority must be independent. Depending on the size and complexity of the department or statutory body, more than three members may be required for the committee to effectively discharge its responsibilities.

#### 3.2 Appointment of the Independent Chair

##### 3.2.1

The department head or governing board of the statutory body must appoint an independent Chair of the Audit and Risk Committee. In doing so, the department head or governing board of the statutory body may either appoint the Chair directly from the panel of pre-qualified individuals maintained through the *Pre-qualification Scheme: Audit and Risk Committee Independent Chairs and Members* or select the Chair from the independent members of the Audit and Risk Committee. The *Pre-qualification Scheme* is discussed in Section 3.3 of this Policy.

##### 3.2.2

When appointing the Chair, the department head or governing board of the statutory body must consider the personal qualities and abilities of the potential Chair to lead discussions, encourage participation of other members, and conduct meetings in a manner that demonstrates a desire to establish effective communications with all stakeholders for continuous improvement.

##### 3.2.3

The Chair must possess a sound understanding of the business of the department or statutory body and the environment in which it operates. It is the responsibility of the department head or governing board of the statutory body to ensure the Chair is provided with all necessary and relevant information regarding the Audit and Risk Committee's responsibilities and the department's or statutory body's operations both prior to and during the Chair's appointment.

### 3.2.4

The Chair must be appointed for a period of at least three (3) years, with a maximum term of four (4) years. This term provides a chair with the opportunity to both contribute effectively and deliver stability in the leadership of the Audit and Risk Committee.

## 3.3 Selection of Independent Members

### 3.3.1

[Department of Premier and Cabinet Circular No. C2009-13](#) establishes the *Pre-qualification Scheme: Audit and Risk Committee Independent Chairs and Members*. Instructions in this Policy relating to the selection and appointment of independent chairs and members of Audit and Risk Committees must be read in conjunction with Circular No. C2009-13 and any accompanying guidelines, as updated from time to time.

### 3.3.2

The department head or governing board of the statutory body must select all independent chairs and members of the Audit and Risk Committee from the panel of pre-qualified individuals maintained by the Department of Commerce through the *Pre-qualification Scheme: Audit and Risk Committee Independent Chairs and Members*. The panel of pre-qualified individuals, and the scheme conditions, are available at the [Department of Commerce website](#).

### 3.3.3

When selecting independent members of the Audit and Risk Committee from the panel of pre-qualified individuals, the department head or governing board of the statutory body must ensure that the individual also satisfies the 'conflict of interest' criteria set out in Section 3.3.4 of this Policy. The department head or governing board of the statutory body must ensure these criteria are applied prior to appointing a pre-qualified individual as an independent member of the Audit and Risk Committee.

### 3.3.4

Pre-qualified individuals who possess one or more of the following relationships cannot be considered independent:<sup>1</sup>

- § has been employed in a senior management role by the department or statutory body, or a related department or statutory body, within the last three years
- § has been employed by the department or statutory body in a position that can exert direct and significant influence over a service provider, within the last three years
- § has performed any services, including advisory roles, for the department or statutory body, or a related department or statutory body, which directly affects the subject matter of the Audit and Risk Committee, within the last three years
- § has a material business or other contractual relationship, other than as a committee member, or any other direct financial interest or material indirect financial interest with the department or statutory body, or a related department or statutory body, which could reasonably be perceived to materially interfere with the Committee member's ability to act in the best interests of the department or statutory body

---

<sup>1</sup> The 'conflict of interest' relationships listed in Section 3.3.4 draw on the independence guidelines set out in Accounting Professional and Ethical Standards Board, [APES110: Code of Ethics for Professional Standards](#), June 2006. Department heads or governing boards of statutory bodies can refer to these standards for further information on independence issues.

- § has acted as an advocate of a material interest on behalf of the department or statutory body, or a related department or statutory body, or currently is, or has been, engaged in litigation or in resolving disputes between the department, or statutory body, and third parties
- § has an immediate family member or close family member who is employed in a senior management role of the department or statutory body, or a related department or statutory body, or is employed in any other position which can exert direct and significant influence over the subject matter of the Audit and Risk Committee.

This is not an exhaustive list of threats to independence, but does prescribe the key relationships that must be avoided. The department head or governing board of the statutory body must ensure appropriate safeguards are in place to eliminate or reduce significant threats to independence to an acceptable level.

#### 3.3.5

The department head or governing board of the statutory body must ensure that adequate procedures are in place to preserve the independence of the independent members of the Audit and Risk Committee.

#### 3.3.6

Independent members of the Audit and Risk Committee must notify the department head or governing board of the statutory body immediately if a real or perceived threat to their independence arises.

#### 3.3.7

Non-executive directors of the governing board of a statutory body are eligible for appointment as independent chairs and members of the Audit and Risk Committee only where they have satisfied the requirements set out in Sections 3.3.2 and 3.3.3 of this Policy.

#### 3.3.8

Current employees of all NSW public sector agencies other than State Owned Corporations cannot serve as independent Members or Chairs of an Audit and Risk Committee. This includes all agencies and employees in the Government service (Public Service Departments, Non-Public Service Divisions and Special Employment Divisions), the Teaching Service, NSW Police and the NSW Health Service. This is to ensure that independence, real and perceived, is maintained.

### 3.4 Selection of Non-Independent Members

#### 3.4.1

The department head or governing board of the statutory body must appoint non-independent members of the Audit and Risk Committee from officers within the department or statutory body. Normally, selection is from senior management.

#### 3.4.2

The department head and the Chief Finance and/or Accounting Officer of either a department or statutory body must not be members of the Audit and Risk Committee.

### 3.4.3

When selecting non-independent members, the department head or governing board of the statutory body must consider the suitability of officers against, and take reasonable steps to ensure that non-independent members appointed to the Audit and Risk Committee collectively possess, the following skills and knowledge:

- § financial literacy
- § broad operational and/or financial management experience
- § understanding of, or experience with, the public sector
- § understanding of the department's or statutory body's operational responsibilities
- § familiarity with risk identification, evaluation and management
- § understanding of internal controls and compliance systems, including information technology systems knowledge of applicable accounting and auditing standards, and major public sector reporting issues
- § familiarity with relevant legislative requirements
- § strong understanding of the roles of internal and external audit.

## 3.5 Rotation of Members

### 3.5.1

The initial term for membership of an Audit and Risk Committee must not exceed four (4) years and should provide an option for reappointment for a further term of maximum four (4) years, particularly for independent members.

### 3.5.2

Any extension of membership on the Audit and Risk Committee must be approved only after the department head or governing board of the statutory body has made an assessment of the member's performance as a committee member. The requirements for performance assessment of Audit and Risk Committee members are set out in Section 4.5 of this Policy.

### 3.5.3

Membership renewal dates must be staggered so significant knowledge is not lost to the Audit and Risk Committee. Ideally, no more than one (1) member should leave the Audit and Risk Committee because of rotation in any one (1) year.

## Core Requirement 4

The Audit and Risk Committee has a Charter that is consistent with the content of the 'model charter'.

### 4.1 Model Charter for Audit and Risk Committees

#### 4.1.1

The department head or governing board of the statutory body must ensure that the Audit and Risk Committee has a Charter that is consistent with the content of the model charter at [Annexe C](#) of this Policy. The model charter sets out 'common' content for Audit and Risk Committee Charters and covers the following structural elements:

- § objective of the Committee
- § authority delegated to the Committee by the department head or governing board of the statutory body
- § composition and tenure
- § roles and responsibilities, including risk management, control framework, external accountability, compliance with applicable laws and regulations, internal audit and external audit
- § responsibilities of members
- § reporting arrangements
- § administrative arrangements, including meetings, attendance at meetings and quorums, dispute resolution, secretariat, conflicts of interest, induction, performance assessment, and review of the charter.

#### 4.1.2

The department head or governing board of the statutory body is required to consider the specific circumstances of the department or statutory body and may, where appropriate, include provisions additional to those set out in the model charter, providing these do not conflict with the model charter.

#### 4.1.3

The department head or governing board of the statutory body must approve the Charter and ensure it has been distributed to all members of the Audit and Risk Committee, including all new appointments.

#### 4.1.4

The Audit and Risk Committee must ensure that:

- § the Charter is formally reviewed by the Audit and Risk Committee periodically, at least annually, to ensure its ongoing relevance, with recommendations for updates approved by the department head or governing board of the statutory body
- § the Charter is sufficiently detailed to ensure there is no ambiguity
- § the Charter has clear guidance on key aspects of the committee's operations.

## 4.2 Audit and Risk Committee Operations

### 4.2.1

The Audit and Risk Committee must meet at least four (4) times in each financial year, i.e. quarterly. Depending on the size and complexity of the department or statutory body, meeting more than four (4) times per year may be necessary in order for the Audit and Risk Committee to effectively perform its roles and discharge its responsibilities.

### 4.2.2

Meetings of the Audit and Risk Committee must be minuted, tabling discussions and results for all work performed.

### 4.2.3

The minutes of meetings of the Audit and Risk Committee must be provided to the department head or governing board of the statutory body within a reasonable time frame, as agreed between the Audit and Risk Committee and the department head or governing board of the statutory body, and normally within two (2) weeks of the meeting date. The agreed time frame must be stated in the Charter.

### 4.2.4

All Audit and Risk Committee members must be promptly provided with all necessary and relevant information in order to fulfil their duties.

### 4.2.5

The Audit and Risk Committee is to have access to operational management when required.

### 4.2.6

The Audit and Risk Committee is able to seek independent, expert advice when required, and may request the department head or governing board of the statutory body to make such expert assistance available.

### 4.2.7

The Audit and Risk Committee must have direct access to the internal and external auditors without operational management being present, and must meet with the internal and external auditors at least annually.

### 4.2.8

The Audit and Risk Committee must have direct access to the Chief Finance and/or Accounting Officer when required.

### 4.2.9

The Audit and Risk Committee has the right to seek explanations and additional information from any employee of the department or statutory body.

### 4.2.10

The Audit and Risk Committee does not have delegated financial responsibility or any management functions.

### 4.2.11

The Audit and Risk Committee has no executive powers.

### 4.3 Reporting Lines: Audit and Risk Committee and Internal Audit

#### 4.3.1

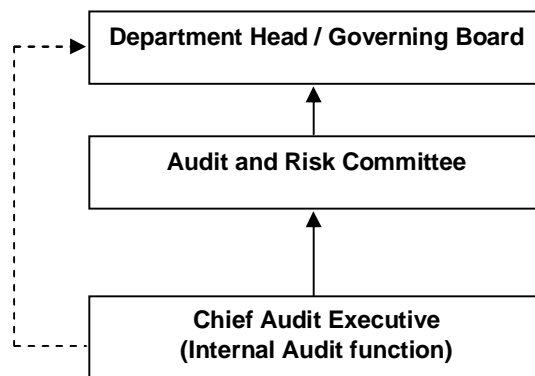
As set out in Section 1.5.1 of this Policy, the department head or governing board of the statutory body must ensure there is a clear separation of operational management from the Internal Audit function.

#### 4.3.2

As set out in Section 1.5.2 of this Policy, to achieve operational independence of the Internal Audit function, the department head or governing board of the statutory body must ensure that the Chief Audit Executive has a dual reporting line. A dual reporting line means that the Chief Audit Executive must:

- § report administratively to the department head or governing board of the statutory body to facilitate day-to-day operations of the Internal Audit function,<sup>1</sup> and
- § report functionally to the Audit and Risk Committee for strategic direction and accountability of the Internal Audit function.

The dual reporting line must be consistent with the following 'reporting line' structure, where the dotted line represents the 'administrative' reporting line, and the bold line represents the 'functional' reporting line:



#### 4.3.3

The department head or governing board of the statutory body must ensure that the dual reporting line structure set out in Section 4.3.2 is included in the Charters for both the Audit and Risk Committee and the Internal Audit function.

### 4.4 Dispute Resolution

#### 4.4.1

The Chair and Members of the Audit and Risk Committee and the department's or statutory body's operational management, including the department head or governing board of the statutory body, must establish and maintain an effective working relationship.

#### 4.4.2

The Chair and Members of the Audit and Risk Committee must seek to resolve differences or concerns with operational management, including the department head or governing board of the statutory body, by way of open negotiation.

<sup>1</sup> In the case of a statutory body, it may be appropriate for the Chief Audit Executive to report administratively to either the chief executive of the statutory body or a delegate director of the board.

#### 4.4.3

Where a disputed matter cannot be resolved, the Chair of the Audit and Risk Committee may make an oral or written request to either the Secretary of NSW Treasury or the Director-General of the Department of Premier and Cabinet requesting access to a central agency arbiter to resolve the dispute.

#### 4.4.4

The central agency may seek to achieve a resolution by mediating between the parties and attempting to reach compromise solutions.<sup>1</sup> The central agency may refer the matter directly to another appropriate authority if such action is warranted, e.g. to report suspected corrupt conduct.

#### 4.4.5

Members of Audit and Risk Committees as public officials are subject to the general principles of conduct that apply to public sector employees. Members must familiarise themselves with the relevant Department of Premier and Cabinet policies and guidelines including:

§ [Code of Conduct and Ethics for Public Sector Executives \(1998\)](#)

§ [Conduct Guidelines for Members of NSW Government Board and Committees \(2001\)](#)

§ [Personnel Handbook, Chapter 8: Model Code of Conduct \(2009\)](#)

§ [Circular C2006-29 SES Grievance and Dispute Resolution Procedures \(2006\)](#).

### 4.5 Performance Assessment of the Audit and Risk Committee

#### 4.5.1

The department head or governing board of the statutory body, in consultation with the Chair of the Audit and Risk Committee, must establish a mechanism to review and report on the performance of the Audit and Risk Committee as a whole, and the performance of the Chair and each member, at least annually. The purpose of the review mechanism is to establish a robust quality assurance and improvement process that ensures the Audit and Risk Committee continues to deliver on its Charter.

#### 4.5.2

The department head or governing board of the statutory body may delegate the performance review function set out in Section 4.5.1 (excluding review of the Chair's performance) to the Audit and Risk Committee Chair, although ultimate responsibility for the integrity of the review mechanism, including the actioning of findings, rests with the department head or governing board of the statutory body.

#### 4.5.3

The review should assess the performance of the Audit and Risk Committee, and the performance of the Chair and members, against the Committee's Charter. The review should be conducted on a self-assessment basis (unless otherwise determined by the department head or governing board of the statutory body) and may include appropriate input from the department head or governing board of the statutory body, operational management, the internal and external auditors, and any other stakeholders as determined by the department head or governing board of the statutory body.

---

<sup>1</sup> Department of Premier and Cabinet (DPC) Circular C2006-29 *SES Grievance and Dispute Resolution Procedures*.

## 4.5.4

In respect of the performance of the Audit and Risk Committee as a whole, the results of the review must be provided to the department head or governing board of the statutory body who should consider the findings and any recommendations of the review and, if required, ensure appropriate action is taken to improve the Audit and Risk Committee's performance.

## 4.5.5

In respect of the performance of independent and non-independent members of the Audit and Risk Committee (excluding the Chair), the results of the review must be provided to the department head or governing board of the statutory body, and the Chair of the Audit and Risk Committee must provide formal feedback to Committee members on their performance.

## 4.5.6

In respect of the performance of the Chair of the Audit and Risk Committee, the results of the review must be provided to the department head or governing board of the statutory body, who must then provide formal feedback to the Chair on his or her performance.

## 4.5.7

In addition to the directions set out in Sections 4.5.5 and 4.5.6, the performance review of independent members of the Audit and Risk Committee (including the Chair) are subject to the relevant parts of the scheme conditions of the *Pre-qualification Scheme: Audit and Risk Committee Independent Chairs and Members*.

#### Useful reference documents

- § [Australian National Audit Office \(ANAO\) \*Public Sector Internal Audit: An Investment in Assurance and Business Improvement, Better Practice Guide\* \(2007\)](#)
- § [Australian Securities Exchange \(ASX\) Corporate Governance Council \*Corporate Governance Principles and Recommendations Second Edition\* \(2007\)](#)
- § [Chartered Accountants \(CA\) \*APES110: Code of Ethics for Professional Standards\* \(2006\)](#)
- § [Department of Premier and Cabinet \(DPC\) \*Performance Review: Internal Audit Capacity in the NSW Public Sector\* \(2008\)](#)
- § [Institute of Internal Auditors \(IIA\) \*International Standards for the Professional Practice of Internal Auditing\* \(2009\)](#)
- § [Institute of Internal Auditors \(IIA\) \*Audit Committees: A Guide to Good Practice\* \(2007\)](#)

## Core Requirement 5

An enterprise risk management process that is appropriate to the department or statutory body has been established and maintained. The enterprise risk management process is consistent with the current Australian/New Zealand Standard (AS/NZS) on risk management.

### 5.1 Risk Management Standards and Definitions

#### 5.1.1

The Government has approved the application of current Australian/New Zealand Standards (AS/NZS) on risk management in the NSW public sector. The current standard is AS/NZS 4360: 2004 *Risk Management* (or 'the Standard').<sup>1</sup> Adoption of the Standard will ensure a common and generally accepted risk management methodology is applied across the NSW public sector.

#### 5.1.2

AS/NZS 4360: 2004 sets out a generic process for organisational risk management. Except where noted, this Policy adopts the Standard's key definitions including:

- § risk is defined as the chance of something happening that will have an impact on objectives - risk may have a positive or negative impact
- § risk management is defined as the culture, processes and structures that are directed towards realising potential opportunities while managing adverse effects
- § risk management framework is the set of elements of an organisation's management system concerned with managing risk
- § risk management policy should clarify the organisation's objectives for and commitment to risk management
- § risk management plans define how risk management is to be conducted throughout the organisation
- § risk management process is defined as the systematic application of management policies, procedures and practices to the tasks of communication, establishing the context, identifying, analysing, evaluating, treating and monitoring and reviewing risk
- § risk assessment is the overall process of risk identification, risk analysis and risk evaluation
- § risk appetite is the level of risk exposure which is considered tolerable and justifiable should it be realised<sup>2</sup>

---

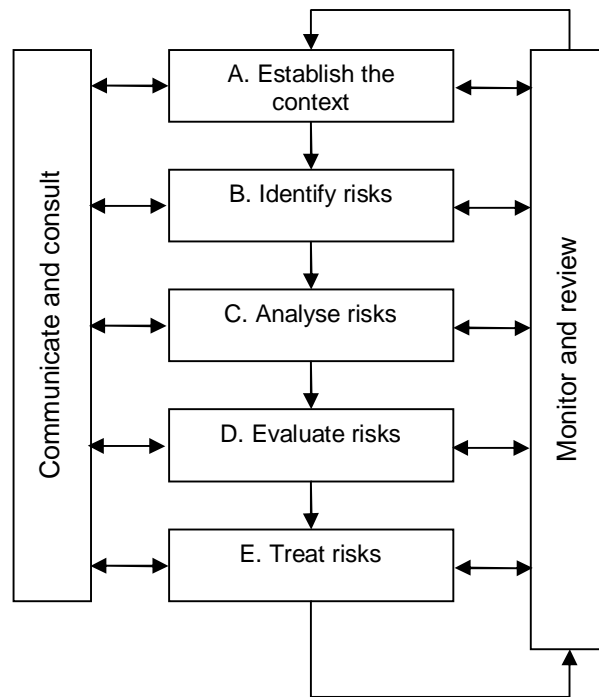
<sup>1</sup> At the time of writing, the International Organisation for Standardization (ISO) was finalising a new international standard on risk management, ISO 31000 *Risk Management - Principles and guidelines on implementation*. ISO 31000 is expected to consolidate existing AS/NZS 4360: 2004 guidance on the risk management process by promoting its implementation as part of an organisation's 'risk management framework'. However, ISO 31000 is also expected to introduce additional requirements. Standards Australia is currently considering a proposal to adopt ISO 31000.

<sup>2</sup> HM Treasury, *The Orange Book: Management of Risk – Principles and Concepts*, October 2004.

- § risk profile is the documented and prioritised overall assessment of the range of specific risks faced by the department or statutory body<sup>1</sup>
- § risk treatment is the process of selection and implementation of measures to modify risk
- § controls are existing processes, policies, devices, practices or other actions that act to minimise negative risks or enhance positive opportunities.

5.1.3

AS/NZS 4360: 2004 sets out the key steps of the risk management process. This Policy adopt the process and related methodology, as illustrated below in Diagram 5.1:



**Diagram 5.1:** Adapted from *Risk Management Overview (AS/NZS 4360:2004)*

The key steps of the risk management process are:

- A. Establishing the external, internal and risk management context for the department or statutory body
- B. Identifying risks, both positive and negative, that could impact on the achievement of the department’s or statutory body’s objectives
- C. Analysing the likelihood and consequence of risks, including the effectiveness of existing controls
- D. Evaluating risks with reference to the level of risk, degree of department’s or statutory body’s control over risk, potential impact of the risk, and importance of the department’s or statutory body’s objectives and activities impacted by the risk
- E. Treatment of risks by identifying and assessing treatment options, and preparing and implementing treatment plans
- F. Monitoring and reviewing the risk management plan to ensure it remains relevant and repeat the risk management cycle regularly for this purpose.

<sup>1</sup> HM Treasury, *The Orange Book: Management of Risk – Principles and Concepts*, October 2004.

## 5.2 Enterprise-wide Risk Management

### 5.2.1

The department head or governing board of the statutory body must ensure that an enterprise-wide risk management (ERM) process that is appropriate to the department or statutory body has been established and maintained within the department or statutory body. The ERM process must be consistent with the methodology set out in AS/NZS 4360: 2004. An ERM process is defined as:

*A structured, consistent and continuous process across the whole organisation for identifying, assessing, deciding on responses to and reporting on opportunities and threats that affect the achievement of its objectives.<sup>1</sup>*

### 5.2.2

When establishing and maintaining an ERM process that is appropriate to the department or statutory body, the department head or governing board of the statutory body must give due regard to the components of better practice of ERM set out in Sections 5.3 - 5.7 of this Policy.<sup>2</sup> A sound ERM process will ensure that risk is defined broadly to include all relevant business risk categories<sup>3</sup>, and that risk management is integrated with a department's or statutory body's strategy-setting, decision-making processes, governance arrangements, policies, plans and procedures.

## 5.3 Risk Management Policy

### 5.3.1

A risk management policy defines and communicates the department's or statutory body's approach to risk, and provides high level guidance on how processes and procedures integrate risk with the everyday work of the department or statutory body. The department head or governing board of the statutory body must ensure that the ERM process gives due regard to the following components of better practice:

- § objectives for managing risk in the department or statutory body
- § linkages with the department's or statutory body's strategic and business plans
- § key accountabilities for managing risk
- § the department's or statutory body's appetite for risk
- § periodic review and continual improvement of the risk management framework and policies
- § communication to employees of the department's or statutory body's approach to risk management
- § linkages with the department's or statutory body's internal audit, compliance and assurance activities.

<sup>1</sup> Institute of Internal Auditors, *IIA Position Paper: The Role of Internal Auditing in Enterprise-Wide Risk Management*, January 2009, p.2.

<sup>2</sup> This discussion of the characteristics of better practice ERM draws on the 'risk management framework' guidelines contained in Comcover, *Risk Management: Better Practice Guide*, June 2008 (copyright Commonwealth of Australia reproduced by permission).

<sup>3</sup> This Policy defines 'all business risk categories' as including (but not confined to): conventional specialist risk categories (such as financial risk, business continuity and disaster recovery, fraud, occupational health and safety, purchasing and procurement, and security), legal, social and economic environment risk, and strategic and service delivery risk.

## 5.4 Risk Management Roles and Responsibilities

### 5.4.1

Effective integration of risk management with a department's or statutory body's governance arrangements, policies and procedures requires clear definition and allocation of accountabilities for risk management within the department or statutory body. The department head or governing board of the statutory body must ensure that the ERM process gives due regard to the following components of better practice:

- § the role of the department head or governing board of the statutory body in approving the risk management policy, determining the risk appetite, approving the risk management plan, ensuring the risk management policy is implemented and reviewed regularly, and reviewing recommendations from the Audit and Risk Committee
- § the role of senior management in developing the risk profile and risk management plan, reviewing business unit risk profiles, reviewing the approach to managing significant risks, reviewing and monitoring completion of treatment plans, and ensuring risk management is implemented in business units
- § the role of the Audit and Risk Committee in reviewing the appropriateness of the risk management process as well as the effectiveness of the process for developing strategic risk management plans (set out in [Annexe C](#) of this Policy)
- § the role of business unit managers in monitoring the risks and risk profile of their areas of responsibility, and ensuring staff are implementing the risk management policy as intended
- § the role of the risk manager (or team) to coordinate and lead implementation of the risk management framework and policy, risk profiles and treatment plans
- § the role of individual staff to apply risk plans in their areas of responsibility by identifying, communicating and responding to expected or emerging risks.

## 5.5 Risk Management Integration

### 5.5.1

Risk management is a critical component of governance arrangements in a department or statutory body and the approach to managing risk should be embedded within a department's or statutory body's planning processes, decision-making structures and operational procedures. The department head or governing board of the statutory body must ensure that the ERM process gives due regard to the following components of better practice:

- § clear articulation and documentation of the linkages between the risk management policy and strategic plans and statements of intent
- § risk management policy should be part of existing business planning, budgeting and reporting processes
- § risk management practices should consider all relevant business risk categories
- § appropriate reflection of the risk appetite in the internal control framework through, for example, financial and other delegations
- § clear communication of risks and risk management practices to internal and external stakeholders, and availability of easy-to-use risk management tools.

## 5.6 Risk Management Review and Evaluation

### 5.6.1

Regular review and evaluation mechanisms are important to assess whether the department's or statutory body's approach to risk management is consistent with its objectives, as well as the extent to which risk appetite, and allocated risk management roles and responsibilities, remain appropriate to the department's or statutory body's strategic directions. The department head or governing board of the statutory body must ensure that the ERM process gives due regard to the following components of better practice:

- § cost-effective mechanisms for monitoring and reviewing both the performance of, and compliance with, the risk management policy
- § formal review of the risk management policy and practice at least annually
- § developing and implementing performance measures that assess the effectiveness of risk treatments and controls that are relevant for the intended audience
- § integrating oversight of risk management with other governing bodies, for example, executive management committees.

## 5.7 Risk Management Culture

### 5.7.1

ERM is built on, and is sustained by, a positive organisational culture that promotes risk management as part of every-day decision making, and supports the acceptance, communication and management of appropriate risk at all levels in the department or statutory body. It is important that senior management take a leadership role in creating an environment that promotes positive risk management behaviour. The department head or governing board of the statutory body must ensure that the ERM process gives due regard to the following components of better practice:

- § clear communication of risk management practices and their benefits
- § encouraging demonstration by senior managers and business unit managers of the application of risk management in day-to-day activities
- § appointment of a senior management sponsor to lead and advocate risk management within the department or statutory body
- § instituting positive reinforcement of effective risk management
- § incorporating measures of risk culture and attitude into organisational climate surveys and performance management systems.

## 5.8 Role of the Audit and Risk Committee<sup>1</sup>

### 5.8.1

The roles and responsibilities of the Audit and Risk Committee with respect to risk management oversight are set out in [Annexe C](#) of this Policy and must cover the following:

- § review whether management has in place a current and appropriate 'enterprise risk management' process, and associated procedures for effective identification and management of the department's or statutory body's financial and business risks, including fraud and corruption
- § review whether a sound and effective approach has been followed in developing strategic risk management plans for major projects or undertakings
- § review the impact of the department's or statutory body's risk management process on its control environment and insurance arrangements
- § review whether a sound and effective approach has been followed in establishing the department's or statutory body's business continuity planning arrangements, including whether disaster recovery plans have been tested periodically
- § review the department's or statutory body's fraud control plan and satisfy itself that the department or statutory body has appropriate processes and systems in place to capture and effectively investigate fraud related information.

### Useful reference documents

- § [Comcover, Risk Management, Better Practice Guide \(2008\)](#)
- § [CPA Australia, Enterprise-Wide Risk Management, CPA Australia's Public Sector Centre of Excellence \(2004\)](#)
- § [Department of Premier and Cabinet \(DPC\), Performance Review: Internal Audit Capacity in the NSW Public Sector \(2008\)](#)
- § [NSW Self Insurance Corporation \(SICorp\), Risk Management Framework Self Assessment Tool \(2008\)](#)
- § [Standards Australia, AS/NZS 4360:2004 Risk Management \(2004\)](#)
- § [Standards Australia, Management Guidelines: Companion to AS/NZS 4360:2004 – HB436:2004 \(2004\)](#)
- § [Treasury Management Fund \(TMF\), TMF Guide to Risk Management: The RCCC Approach \(2005\)](#)

---

<sup>1</sup> This section is extracted from ANAO Better Practice Guide, *Public Sector Audit Committees*, 2005 (copyright Commonwealth of Australia reproduced by permission).

## Core Requirement 6

The operation of the Internal Audit function is consistent with IIA *International Standards for the Professional Practice of Internal Auditing*. In addition, the following requirements must be met:

- the Chief Audit Executive has implemented a risk based audit methodology for assessing and responding to audit findings, and this approach has been endorsed by the Audit and Risk Committee
- the Chief Audit Executive has ensured a risk rating has been provided on every audit finding, and those audit findings considered by the Chief Audit Executive to be the most significant have been reviewed by the Audit and Risk Committee
- the Chief Audit Executive has recommended a course of action for every audit finding, and these actions have been referred to operational management for response
- the department head or governing board of the statutory body has ensured that operational management has prepared an 'agreed action plan' for every internal audit
- the department head or governing board of the statutory body has ensured that operational management has reported and tracked the implementation of 'agreed action plans' to both the Audit and Risk Committee and the department head or governing board of the statutory body to ensure all agreed actions are implemented within agreed time frames.

### 6.1 Internal Audit Standards

#### 6.1.1

The Government has approved the application of the Institute of Internal Auditors (IIA) *International Standards for the Professional Practice of Internal Auditing* (the IIA Standards) in the NSW public sector. The IIA Standards, and related professional practice guidelines, are available from the [Institute of Internal Auditors website](#).

#### 6.1.2

The department head or governing board of the statutory body must ensure that the Internal Audit function, as defined in this Policy, operates in accordance with the IIA Standards, unless the IIA Standards are in conflict with the *Internal Audit and Risk Management Policy* or any related directions issued under Treasurer's Direction.

## 6.2 Additional Internal Audit Requirements - Audit Reports

### 6.2.1

The audit report is the key means of communicating the findings and recommendations of internal audit services. It is critical that all stakeholders have confidence in the accuracy and validity of audit findings, and that appropriate standards are applied to ensure that audit recommendations are prioritised, action-oriented and cost-effective to implement. In addition to the standards set out in the IIA Standards, the department head or governing board of the statutory body must ensure that the Internal Audit function, as defined in this Policy, operates in accordance with the requirements for the reporting and monitoring of internal audit activities set out in Sections 6.3 - 6.7.

## 6.3 Audit Reporting Standards

### 6.3.1

The Chief Audit Executive must report to the Audit and Risk Committee those internal audit findings and related recommendations that are assessed to be the most significant using the risk based audit methodology set out in section 6.4 of this Policy. The Chief Audit Executive must also ensure that the Audit and Risk Committee has access to all internal audit findings and related recommendations when required.

### 6.3.2

The Chief Audit Executive must develop and maintain policies and procedures for the reporting of internal audit findings and recommendations in the department or statutory body. The following better practice standards can be used as guidelines for these policies and procedures.

The report:

- § contains an overall audit conclusion and rating related to the audit objective(s)
- § is prepared in accordance with a stipulated report template
- § is drafted and finalised within stipulated timeframes
- § meets length stipulations
- § includes comments from the sponsor
- § includes an action plan, including the individual responsible and timeframe for implementing agreed recommendations.

## 6.4 Risk Rating of Audit Findings

### 6.4.1

The Chief Audit Executive must ensure that the Internal Audit function adopts a risk based audit methodology for assessing and responding to audit issues. The methodology should be consistent with the current risk standard, as defined in Section 5.1 of this Policy.

### 6.4.2

The Audit and Risk Committee must approve the risk based audit methodology. Once approved, the methodology must be the basis for protocols relating to reporting of audit findings, monitoring the implementation of agreed actions, and the follow-up of outstanding agreed actions.

#### 6.4.3

The Chief Audit Executive must ensure that every audit finding is categorised and prioritised according to the risk the audit finding represents to the department or statutory body if the recommendation(s) related to the finding are not implemented.

#### 6.4.4

The Chief Audit Executive must ensure that a common, easily understood system for risk categorisation is used to communicate the relative importance of risk ratings of findings to the Audit and Risk Committee, the department head or governing board of the statutory body, and operational management, e.g. alpha grades (high, medium, low), traffic light colours (red, yellow, green) etc.

#### 6.4.5

The Audit and Risk Committee must review the audit findings and related recommendations that have been assessed as the most significant according to the risk the audit finding represents to the department or statutory body if the recommendation(s) related to the finding are not implemented.

### 6.5 Agreed Action Plans

#### 6.5.1

The Chief Audit Executive must recommend a course of action for every audit finding.

#### 6.5.2

The Chief Audit Executive must ensure that the recommended actions are referred to operational management for formal response. Operational management has the right to reject recommended actions on reasonable grounds. However, the Chief Audit Executive must report to the Audit and Risk Committee where agreement cannot be reached.

#### 6.5.3

The department head or governing board of the statutory body must ensure that operational management prepares an 'agreed action plan' for every internal audit. The agreed action plan must assign responsibility for implementation to individuals within the department or statutory body. The following better practice standards can be used as guidelines for agreed action plan timeframes:

- § actions to address high risk findings specify an agreed implementation timeframe between one (1) and three (3) months
- § actions to address medium risk findings specify an agreed implementation timeframe between three (3) and six (6) months
- § actions to address low risk findings specify an agreed implementation timeframe between six (6) and twelve (12) months.

### 6.6 Monitoring of Agreed Action Plans

#### 6.6.1

The department head or governing board of the statutory body must ensure that all agreed actions are implemented within agreed timeframes. To achieve this, the department head or governing board of the statutory body must ensure that operational management monitors progress of, and reports on, the implementation of 'agreed action plans' to both the Audit and Risk Committee and the department head or governing board of the statutory body.

#### 6.6.2

The Chief Audit Executive must, on advice from the Audit and Risk Committee, monitor progress in implementing 'agreed action plans', by undertaking follow-up audits based on the risks posed to the department or statutory body if agreed actions are not implemented in a timely manner, and report on progress to the Audit and Risk Committee.

## 6.6.3

Where the Audit and Risk Committee is not satisfied with progress in implementing agreed actions, the Audit and Risk Committee must refer the concerns to operational management, including the department head or governing board of the statutory body, so that operational management is made fully aware of the risks posed to the department or statutory body.

## 6.7 Internal Audit Manual

## 6.7.1

The department head or governing board of the statutory body must ensure that the Chief Audit Executive develops and maintains an Internal Audit Manual for the Internal Audit function.

## 6.7.2

Where the Internal Audit function is established using an out-sourced service delivery model (as defined in Section 1.2.4 of this Policy), the department head or governing board of the statutory body must ensure the contract for internal audit services specifies that the external third party provider will:

- § be consulted in the development and/or maintenance of the Internal Audit Manual
- § apply audit methodologies that accord with IIA Standards
- § make the audit methodologies used accessible to the department or statutory body (subject to any licensing or other restrictions that may be in place).

## 6.7.3

The Audit and Risk Committee must approve the Internal Audit Manual.

## 6.7.4

The Internal Audit Manual must be consistent with professional practices set out in the IIA Standards, and should cover the following structural elements:

**1. General Policies and Standards:**

- § Audit Charter
- § Audit Standards and Guiding Principles
- § Audit and Risk Committee Charter

**3. Audit Planning:**

- § Planning
- § Strategic Audit Plan
- § Annual Audit Plan
- § Field Audit Plan

**5. Ongoing Audit Engagements and Development Audits:**

- § Audit Objectives
- § Audit Approach
- § Audit Working Papers

**2. Personnel:**

- § Personnel
- § Time Usage Analysis

**4. Audit Methodology:**

- § The Audit Cycle - Summary
- § Risk and Control Analysis (RACA)
- § Audit Programs
- § Working Papers - General
- § Current Working Papers
- § Audit Reports
- § Working Paper Review
- § Audit Sampling

**6. Engagement Evaluations and Performance Reviews:**

- § Performance Reviews

## 6.7.5

The department head or governing board of the statutory body must ensure policies and procedures for the retention, storage and management of internal audit documentation are developed and maintained. As required by [Treasury Circular NSWTC 07/14 \*Ownership of Internal Audit Documentation\*](#), all internal audit documentation is to remain the property of the audited department or statutory body, including where the internal audit services are performed by an external third party provider.

## Useful reference documents

- § [Australian National Audit Office \(ANAO\), \*Public Sector Internal Audit: An Investment in Assurance and Business Improvement\*, Better Practice Guide \(2007\)](#)
- § [Department of Premier and Cabinet \(DPC\), \*Performance Review: Internal Audit Capacity in the NSW Public Sector\* \(2008\)](#)
- § [Institute of Internal Auditors \(IIA\) \*International Standards for the Professional Practice of Internal Auditing\* \(2009\)](#)

## Annexe A

### Better Practice Framework for Internal Audit

Whole-of-Government	
<b>1. Governance</b> (internal audit policy and regulation)	<b>1.1. Internal audit policy and regulatory expectations:</b> Clear internal audit policy direction and leadership, practice standards set and mechanism to ensure compliance with those standards. <b>1.2. Compliance assurance:</b> Monitoring and regulation of compliance with legislation and policy.
<b>Agency</b>	
<b>2. Governance</b>	<b>2.1. Independent audit committee:</b> Independent Chair and other independent members with independent panel appointing members. <b>2.2. Independence of the internal audit function:</b> A quality internal audit function requires independence from operational management and knowledge to effectively manage the function. <b>2.3. Internal audit reporting:</b> Established methodologies for control effectiveness assessment, audit findings risk rating to determine issues for management action; and active monitoring and enforcement of agreed solutions.
<b>3. Risk management</b>	<b>3.1. Risk management oversight:</b> Charter for the Audit Committee includes oversight of risk management. <b>3.2. Integrated risk management practices:</b> Strategic and operational risk management is integrated across the organisation and with internal audit and other assurance activities. <b>3.3. Risk based audit:</b> Internal audit activities are based on the enterprise's integrated risk management and planned controls.
<b>4. Control audit</b>	<b>4.1. Audit activities:</b> Appropriate range of efficient activities for effective achievement of internal audit objectives. Activities encompass hard and soft controls, pre-emptive audits for change risks, performance improvement and coordination with other assurance activities. <b>4.2. Audit resources:</b> Auditors and the staff managing an internal audit function have both the inherent skills (e.g. inter-personal, analytical and communication) and knowledge (e.g. audit, business and specialist) to effectively undertake internal audit services. <b>4.3. Audit processes and systems:</b> Documented audit practices based on externally recognised better practice. Relevant technology is utilised to maximise audit and control effectiveness. Partnership approach between audit and management to improve performance and achieve business objectives. <b>4.4. Currency of audit knowledge:</b> Access to and active use of audit "thought leadership", exchange and sharing of knowledge, expertise and audit strategies to ensure ongoing effectiveness of the audit function.

## Annexe B

### Model Internal Audit Charter<sup>1</sup>

The Internal Audit function of NSW departments and statutory bodies is required to have a charter that is consistent with the content of the 'model charter'. The Chief Audit Executive is required to review, in consultation with the department head or governing board of the statutory body and the Audit and Risk Committee, their existing Internal Audit Charter against this model. In doing so it is important that each department or statutory body consider carefully its particular circumstances, as there may be *additional* agency specific requirements that must also be addressed.

The purpose of this Internal Audit Charter is to address the role, responsibilities, authorisation, activities and reporting relationships of the Internal Audit function. The charter should be reviewed on a regular basis to ensure that it is consistent with changes in the financial, risk management and governance arrangements of the department or statutory body, and reflects developments in Internal Audit professional practices.

#### Introduction

The [department head or governing board of the statutory body] has established the [name of internal audit unit] as a key component of the [department or statutory body]'s governance framework.

This charter provides the framework for the conduct of the Internal Audit function in the [department or statutory body] and has been approved by the [department head or governing board of the statutory body] on the advice of the Audit and Risk Committee.

#### Purpose of internal audit

Internal audit is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.<sup>2</sup>

Internal audit provides an independent and objective review and advisory service to:

- § provide assurance to the [department head or governing board of the statutory body], and the Audit and Risk Committee, that the [department or statutory body]'s financial and operational controls, designed to manage the organisation's risks and achieve the entity's objectives, are operating in an efficient, effective and ethical manner, and
- § assist management in improving the entity's business performance.

<sup>1</sup> This Model Internal Audit Charter is a modified version of the model charter set out in the Australian National Audit Office (ANAO) Better Practice Guide *Public Sector Internal Audit: An Investment in Assurance and Business Improvement*, September 2007. Copyright Commonwealth of Australia reproduced by permission.

<sup>2</sup> As defined by the International Standards for the Professional Practice of Internal Audit (IIA) (2009). Where relevant, sections of this Charter also incorporate other elements of the International Standards for the Professional Practice of Internal Auditing.

## Independence

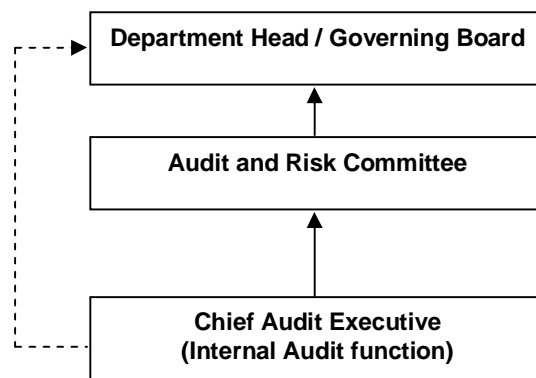
Independence is essential to the effectiveness of the Internal Audit function. Internal audit activity must be independent, and internal auditors must be objective in performing their work. Internal auditors must have an impartial, unbiased attitude and avoid any conflicts of interest.

The Internal Audit function has no direct authority or responsibility for the activities it reviews. The Internal Audit function has no responsibility for developing or implementing procedures or systems and does not prepare records or engage in original line processing functions or activities [except as noted below].

The Internal Audit function is responsible on a day to day basis to the Chief Audit Executive.

The Internal Audit function, through the Chief Audit Executive, reports functionally to the Audit and Risk Committee on the results of completed audits, and for strategic direction and accountability purposes, and reports administratively to the [department head or governing board of the statutory body] to facilitate day to day operations.

The following reporting line is prescribed:



## Authority and confidentiality

Internal auditors are authorised to have full, free and unrestricted access to all functions, premises, assets, personnel, records, and other documentation and information that the Chief Audit Executive considers necessary to enable the Internal Audit function to meet its responsibilities.

All records, documentation and information accessed in the course of undertaking internal audit activities are to be used solely for the conduct of these activities. The Chief Audit Executive and individual internal audit staff are responsible and accountable for maintaining the confidentiality of the information they receive during the course of their work.

All internal audit documentation is to remain the property of the audited [department or statutory body], including where internal audit services are performed by an external third party provider.

## Roles and responsibilities

The Internal Audit function must evaluate and contribute to the improvement of governance, risk management, and control processes using a systematic and disciplined approach.

In the conduct of its activities, the Internal Audit function will play an active role in:

- § developing and maintaining a culture of accountability and integrity
- § facilitating the integration of risk management into day-to-day business activities and processes, and
- § promoting a culture of cost-consciousness, self-assessment and adherence to high ethical standards.

Internal audit activities will encompass the following areas:

**Audit activities** including audits with the following orientation:

### ***Risk Management***

- § evaluate the effectiveness of, and contribute to the improvement in, risk management processes
- § provide assurance that risk exposures relating to the organisation's governance, operations, and information systems are correctly evaluated, including:
  - reliability and integrity of financial and operational information
  - effectiveness, efficiency and economy of operations, and
  - safeguarding of assets
- § evaluate the design, implementation, and effectiveness of the organisation's ethics-related objectives, programs, and activities
- § assess whether the information technology governance of the organisation sustains and supports the organisation's strategies and objectives

### ***Compliance***

- § compliance with applicable laws and regulations

### ***Performance improvement***

- § the efficiency, effectiveness, and economy of the entity's business systems and processes.

## Advisory services

The Internal Audit function can advise the [department or statutory body]'s management on a range of matters including:

### ***New programs, systems and processes***

- § providing advice on the development of new programs and processes and/or significant changes to existing programs and processes including the design of appropriate controls

### ***Risk management***

- § assisting management to identify risks and develop risk mitigation and monitoring strategies as part of the risk management framework

### ***Fraud control***

- § evaluate the potential for the occurrence of fraud and how the organisation manages fraud risk
- § assisting management to investigate fraud, identify the risks of fraud and develop fraud prevention and monitoring strategies.

### Audit support activities

The Internal Audit function is also responsible for:

- § assisting the Audit and Risk Committee to discharge its responsibilities
- § providing secretarial support to the Audit and Risk Committee
- § monitoring the implementation of agreed recommendations
- § disseminating across the entity better practice and lessons learnt arising from its audit activities.

### Scope of internal audit activity

Internal audit reviews cover all programs and activities of the [department or statutory body] together with associated entities, as provided for in relevant business agreements, memorandum of understanding or contracts. Internal audit activity encompasses the review of all financial and non-financial policies and operations.

### Standards

Internal audit activities will be conducted in accordance with relevant professional standards including:

- § International Standards for the Professional Practice of Internal Auditing issued by the Institute of Internal Auditors
- § Standards issued by Standards Australia and the International Standards Organisation.

In the conduct of internal audit work, internal audit staff will:

- § comply with relevant professional standards of conduct
- § possess the knowledge, skills and technical proficiency relevant to the performance of their duties
- § be skilled in dealing with people and communicating audit, risk management and related issues effectively
- § exercise due professional care in performing their duties.

### Relationship with external audit

Internal and external audit activities will be coordinated to help ensure the adequacy of overall audit coverage and to minimise duplication of effort.

Periodic meetings and contact between internal and external audit shall be held to discuss matters of mutual interest and facilitate coordination.

External audit will have full and free access to all internal audit plans, working papers and reports.

### Planning

The Chief Audit Executive will prepare, for the Audit and Risk Committee's consideration, an internal audit annual audit work plan in a form agreed with the Committee.

### Reporting

The Chief Audit Executive will report to each meeting of the Audit and Risk Committee on:

- § audits completed
- § progress in implementing the annual audit work plan, and
- § the implementation status of agreed internal and external audit recommendations.

The Internal Audit function will also report to the Audit and Risk Committee at least annually on the overall state of internal controls in the [department or statutory body] and any systemic issues requiring management attention based on the work of the Internal Audit function [and other assurance providers].

### Administrative arrangements

Any change to the position of the Chief Audit Executive, [or, where the Internal Audit function uses an outsourced service delivery model, the external service provider] will be approved by the [department head or governing board of the statutory body] in consultation with the Audit and Risk Committee.

The Chief Audit Executive will arrange for an internal review, at least annually, and a periodic independent review, at least every five (5) years, of the efficiency and effectiveness of the operations of the Internal Audit function.

### Review of the charter

This charter will be reviewed at least annually by the Audit and Risk Committee. Any substantive changes will be formally approved by the [department head or governing board of the statutory body] on the recommendation of the Audit and Risk Committee.

## Annexe C

### Model Audit and Risk Committee Charter<sup>1</sup>

Audit and Risk Committees of NSW departments and statutory bodies are required to have a Charter that is consistent with the content of the 'model charter'. The department head or governing board of the statutory body and the Audit and Risk Committee are therefore required to review their existing charters against this model. In doing so it is important that each department or statutory body consider carefully its particular circumstances, as there may be additional agency specific requirements that must also be addressed.

The [department head or governing board of the statutory body] has established the Audit and Risk Committee ('the Committee') in compliance with Treasury Circular NSW TC 09/08 August 2009.

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

#### Objective

The objective of the Committee is to provide independent assistance to the [department head or governing board of the statutory body] by overseeing and monitoring the [department or statutory body]'s governance, risk and control frameworks, and its external accountability requirements.

#### Authority

The [department head or governing board of the statutory body] 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 [department head or governing board of the statutory body], at committee meetings
- § obtain external legal or other professional advice, as considered necessary to meet its responsibilities, at the [department or statutory body]'s expense.

#### Composition and tenure

The Committee will consist of at least three (3) members, and no more than five (5) members, appointed by the [department head or governing board of the statutory body].<sup>2</sup> A majority of the Committee members must be independent members.<sup>3</sup> The [department head or governing board of the statutory body] will appoint the Chair of the Committee. The Chair must be an independent member. The Chair is counted as one member of the Committee.

<sup>1</sup> This Model Audit and Risk Committee Charter is a modified version of the model charter set out in the Australian National Audit Office (ANAO) *Better Practice Guide: Public Sector Audit Committees*, February 2005. Copyright Commonwealth of Australia reproduced by permission.

<sup>2</sup> Requirements relating to the composition of the Audit and Risk Committee are located in the Policy at Sections 2.1 and 3.1.

<sup>3</sup> Requirements relating to 'independent members' are located in the Policy at Sections 3.1 – 3.4

Members will be appointed for an initial period not exceeding four (4) years,<sup>1</sup> after which they will be eligible for extension or re-appointment for a further maximum term of four (4) years, after a formal review of their performance.

The [department head or governing board of the statutory body], Chief Finance and Accounting Officers and the Chief Audit Executive will not be members of the Committee, but may attend meetings as observers as determined by the Chair.

The members, taken collectively, will have a broad range of skills and experience relevant to the operations of the [department or statutory body]. 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.<sup>2</sup>

### Roles and responsibilities

The Committee has no executive powers.<sup>3</sup>

The Committee is directly responsible and accountable to the [department head or governing board of the statutory body] 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 [department or statutory body] rests with the [department head or governing board of the statutory body].

The responsibilities of the Committee may be revised or expanded in consultation with, or as requested by, the [department head or governing board of the statutory body] from time to time.

The Committee's responsibilities are to:

### Risk management

- § review whether management has in place a current and appropriate 'enterprise risk management' process, and associated procedures for effective identification and management of the [department or statutory body]'s financial and business risks, including fraud and corruption<sup>4</sup>
- § review whether a sound and effective approach has been followed in developing strategic risk management plans for major projects or undertakings
- § review the impact of the [department or statutory body]'s risk management process on its control environment and insurance arrangements
- § review whether a sound and effective approach has been followed in establishing the [department or statutory body]'s business continuity planning arrangements, including whether disaster recovery plans have been tested periodically
- § review the [department or statutory body]'s fraud control plan and satisfy itself that the [department or statutory body] has appropriate processes and systems in place to capture and effectively investigate fraud related information.

<sup>1</sup> Requirements relating to the rotation of members are located in the Policy at Section 3.5.

<sup>2</sup> Requirements relating to appointment of independent members and non-independent members differ, and are located in the Policy at Sections 3.2 - 3.4.

<sup>3</sup> Requirements relating to defined reporting lines are located in the Policy at Sections 1.5 and 4.3.

<sup>4</sup> Requirements relating to the Committee's oversight of risk management are located in the Policy at Sections 3.2 - 3.4.

### 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
- § 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.

### External accountability

- § review the financial statements and provide advice to the [department head or governing board of the statutory body] (including whether appropriate action has been taken in response to audit recommendations and adjustments), and recommend their signing by the [department head or governing board of the statutory body]
- § satisfy itself that the financial statements are supported by appropriate management signoff on the statements and on the adequacy of the systems of internal controls
- § review the processes in place designed to ensure that financial information included in the [department or statutory body]'s annual report is consistent with the signed financial statements
- § satisfy itself that the [department or statutory body] has a performance management framework that is linked to organisational objectives and outcomes.

### Compliance with applicable laws and regulations

- § determine whether management has appropriately considered legal and compliance risks as part of the [department or statutory body]'s risk assessment and management arrangements
- § review the effectiveness of the system for monitoring the [department or statutory body]'s compliance with applicable laws and regulations, and associated government policies.

### Internal audit

- § act as a forum for communication between the [department head or governing board of the statutory body], senior management and internal and external audit
- § review the internal audit coverage and annual work plan, ensure the plan is based on the [department or statutory body]'s risk management plan, and recommend approval of the plan by the [department head or governing board of the statutory body]
- § advise the [department head or governing board of the statutory body] on the adequacy of internal audit resources to carry out its responsibilities, including completion of the approved internal audit plan
- § oversee the coordination of audit programs conducted by internal and external audit and other review functions

- § review all audit reports and provide advice to the [department head or governing board of the statutory body] on significant issues identified in audit reports and action taken on issues raised, including identification and dissemination of good practice
- § monitor management's implementation of internal audit recommendations
- § review the internal audit charter to ensure appropriate organisational structures, authority, access and reporting arrangements are in place
- § periodically review the performance of internal audit
- § provide advice to the [department head or governing board of the statutory body] on the appointment or replacement of the Chief Audit Executive [in the case of an in-house internal audit function where that function is the predominant role of that officer], and/or recommend to the [department head or governing board of the statutory body] the appointment or replacement of the internal auditors [in the case of an outsourced internal audit function]. [Amend as appropriate].

#### External audit

- § act as a forum for communication between the [department or statutory body], senior management and internal and external audit
- § provide input and feedback on the financial statements and performance audit coverage proposed by external audit and provide feedback on the audit services provided
- § review all external plans and reports in respect of planned or completed audits and monitor management's implementation of audit recommendations
- § provide advice to the [department head or governing board of the statutory body] on action taken on significant issues raised in relevant external audit reports and better practice guides.

#### Responsibilities of members

Members of the Committee are expected to understand and observe the legal requirements of Treasury Circular NSW TC 09/08 August 2009. Members are also expected to:

- § contribute the time needed to study and understand the papers provided
- § apply good analytical skills, objectivity and good judgement
- § express opinions frankly, ask questions that go to the fundamental core of the issue and pursue independent lines of enquiry.

#### Reporting

The Committee will regularly, but at least once a year, report to the [department head or governing board of the statutory body] on its operation and activities during the year. The report should include:

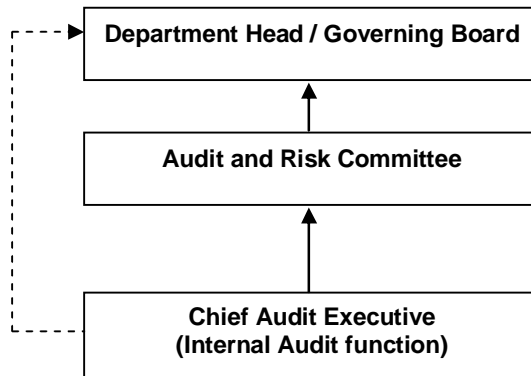
- § a summary of the work the Committee performed to fully discharge its responsibilities during the preceding year
- § a summary of the [department or statutory body]'s progress in addressing the findings and recommendations made in internal and external reports
- § an overall assessment of the [department or statutory body]'s risk, control and compliance framework, including details of any significant emerging risks or legislative changes impacting the [department or statutory body]
- § details of meetings, including the number of meetings held during the relevant period, and the number of meetings each member attended.

The Committee may, at any time, report to the [department head or governing board of the statutory body] 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 [department head or governing board of the statutory body].

**Reporting Lines**

The Committee must at all times ensure it maintains a direct reporting line to and from internal audit and act as a mechanism for internal audit to report to the [department head or governing board of the statutory body] on functional matters.<sup>1</sup>

The following reporting line is prescribed:



**Administrative arrangements**

**Meetings**

The Committee will meet at least four (4) times per year.<sup>2</sup> A special meeting may be held to review the [department or statutory body]’s annual financial statements.

The Chair is required to call a meeting if requested to do so by the [department head or governing board of the statutory body], or another Committee member.

A meeting plan, including meeting dates and agenda items, will be agreed by the Committee each year. The meeting plan will cover all of the Committee’s responsibilities as detailed in this charter.

**Attendance at meetings and 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 Chief Audit Executive and external audit representatives will be invited to attend each meeting, unless requested not to do so by the Chair of the Committee. The Committee may also request the Chief Finance Officer or other employees attend committee meetings or participate for certain agenda items.

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

<sup>1</sup> Requirements relating to reporting lines are located in the Policy at Sections 1.5 and 4.3

<sup>2</sup> Requirements relating to meetings are located in the Policy at Section 4.2.

The [department head or governing board of the statutory body] may be invited to attend committee meetings to participate in specific discussions or provide strategic briefings to the Committee as determined by the Chair.

#### Dispute Resolution

Members of the Committee and the [department or statutory body]'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 [department head or governing board of the statutory body], the Chair may, as a last resort, refer the matter to a central agency to be dealt with independently.<sup>1</sup>

#### Secretariat

The [department head or governing board of the statutory body] will appoint a person to provide secretariat support to the Committee. The Secretariat will ensure the agenda for each meeting 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 must be approved by the Chair and circulated within [agreed time frame] of the meeting to each member and committee observers, as appropriate.

#### Conflicts of interest

Once a year the Committee members will provide written declarations to the [department head or governing board of the statutory body] stating they do not have any conflicts of interest that would preclude them from being members of the Committee.<sup>2</sup>

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 conflicts of interest should be appropriately minuted.

Where members or observers at committee meetings are deemed to have a real, or perceived, conflict of interest it may be appropriate that they are excused from committee deliberations on the issue where a conflict of interest exists.

#### Induction

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

#### Assessment arrangements

The [department head or governing board of the statutory body], 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 [department head or governing board of the statutory body]) with appropriate input sought from the [department head or governing board of the statutory body], the internal and external auditors, management and any other relevant stakeholders, as determined by the [department head or governing board of the statutory body].

---

<sup>1</sup> Requirements relating to the dispute resolution mechanism are located in the Policy at Section 4.4.

<sup>2</sup> Requirements for independent members, including the relationships that give rise to conflicts of interest, are contained in the Policy at Sections 3.1 - 3.3.

**Review of charter**

At least once a year the Committee will review this Charter. This review will include consultation with the [department head or governing board of the statutory body].

Any substantive changes to this Charter will be recommended by the Committee and formally approved by the [department head or governing board of the statutory body].

Reviewed by Chair of Audit and Risk  
Committee (Sign and Date)

Reviewed by the Department Head or in  
accordance with a resolution of the Governing  
Board of the Statutory Body (Sign and Date)

---

---

## Annexe D

### Attestation Statement Template (Internal Audit and Risk Management Policy Compliance)

Treasury Circular NSW TC 09/08 August 2009 requires the department head or governing board of the statutory body to attest to compliance with the 'core requirements' set out in the Policy annually.

The department head or governing board of the statutory body must use the relevant Attestation Statement Template (either Template D1 or D2) to attest that for the relevant reporting period the department or statutory body is compliant with the 'core requirements'.

#### Meaning of Compliant

'Compliant' means that for *each* core requirement *either* the department or statutory body has the core requirement 'in place' (for the financial year ending on or after 30 June 2010) or 'in operation' (for financial years ending on or after 30 June 2011) *or* the department or statutory body has a determination from the Portfolio Minister that the circumstances for an exception to the core requirement exist in the department or statutory body for the relevant reporting period.

#### Attesting for Controlled Entities

Where a department or statutory body has '*control*' of an entity (or subsidiary), as defined in the Australian Accounting Standards, the parent department or statutory body should consider the impact of the controlled entity (or subsidiary) when making the declaration. The parent entity may elect to include a controlled entity (or subsidiary) in the declaration. Where a parent entity elects to do so, it should declare which controlled entities (or subsidiaries) on behalf of which the attestation is made. Where a controlled entity (or subsidiary) is scheduled under annual reporting legislation to prepare an annual report, the controlled entity (or subsidiary) must make its own declaration.

Template D1: No Exceptions

Internal Audit and Risk Management Attestation for the  
200X-201X Financial Year for [department or statutory  
body]

*In the case of compliance with no exceptions use the following:*

I, [department head or governing board of the statutory body] am of the opinion that the [department or statutory body] has internal audit and risk management processes in place that are, in all material respects, compliant with the core requirements set out in Treasury Circular NSW TC 09/08 *Internal Audit and Risk Management Policy*. These processes provide a level of assurance that enables the senior management of [department or statutory body] to understand, manage and satisfactorily control risk exposures.

I, [department head or governing board of the statutory body] am of the opinion that the Audit and Risk Committee for [department or statutory body] is constituted and operates in accordance with the independence and governance requirements of Treasury Circular NSW TC 09/08 . The Chair and Members of the Audit and Risk Committee are:

- § independent Chair (term of appointment)
- § independent Member 1 (term of appointment) etc.
- § non-independent Member 1 (term of appointment) etc.

[Where a department or statutory body has 'control' of an entity (or subsidiary), as defined in the Australian Accounting Standards, and the department or statutory body elects to include a controlled entity (or subsidiary) in the Attestation, use the following wording to declare each of the controlled entities (or subsidiaries) on behalf of which the attestation statement is made:

I, [department head or governing board of the statutory body] declare that this Internal Audit and Risk Management Attestation is made on behalf of the following controlled entities (or subsidiaries):

- § controlled entity (or subsidiary) 1
- § controlled entity (or subsidiary) 2 etc.]

Department Head or in accordance with a  
resolution of the Governing Board of the  
Statutory Body

(Sign and Date)

Department or Statutory Body Contact Officer

(Position and contact details)

---

Template D2: Exceptions

Internal Audit and Risk Management Attestation for the 200X-201X Financial Year for [department or statutory body]

In the case of compliance with exceptions use the following:

I, [department head or governing board of the statutory body] am of the opinion that the [department or statutory body] has internal audit and risk management processes in place that are, excluding the exceptions described below, compliant with the core requirements set out in Treasury Circular NSW TC 09/08 *Internal Audit and Risk Management Policy*.

I, [department head or governing board of the statutory body] am of the opinion that the internal audit and risk management processes for [department or statutory body] depart from the following core requirements set out in Treasury Circular NSW TC 09/08 and that (a) the circumstances giving rise to these departures have been determined by the Portfolio Minister and (b) the [department or statutory body] has implemented [or is implementing] the following practicable alternative measures that will achieve a level of assurance equivalent to the requirement:

Ministerially Determined Departure	Reason for Departure and Description of Practicable Alternative Measures Implemented
<ul style="list-style-type: none"> <li>• Core Requirement X</li> </ul>	<ul style="list-style-type: none"> <li>• Detailed description of circumstances giving rise to departure(s)</li> <li>• Detailed description of the alternative measures implemented / being implemented to achieve equivalent level of assurance</li> </ul>
<p><i>The determination by the Portfolio Minister for [department or statutory body] in respect of these departures, dated XX month 20XX, is appended to this attestation statement.</i></p>	

These processes, including the practicable alternative measures [being] implemented, provide a level of assurance that enables [will enable] the senior management of [department or statutory body] to understand, manage and satisfactorily control risk exposures.

I, [department head or governing board of the statutory body] am of the opinion that the Audit and Risk Committee [or shared service / policy cluster equivalent] for [department or statutory body] is constituted and operate[s] in accordance with the independence and governance requirements of Treasury Circular NSW TC 09/08 . The Chair and Members of the Audit and Risk Committee are:

- § independent Chair (term of appointment)
- § independent Member 1 (term of appointment) etc.
- § non-independent Member 1 (term of appointment) etc.

[Where a department or statutory body has 'control' of an entity (or subsidiary), as defined in the Australian Accounting Standards, and the department or statutory body elects to include a controlled entity (or subsidiary) in the Attestation, use the following wording to declare each of the controlled entities (or subsidiaries) on behalf of which the attestation statement is made:

I, [department head or governing board of the statutory body] declare that this Internal Audit and Risk Management Attestation is made on behalf of the following controlled entities (or subsidiaries):

§ controlled entity (or subsidiary) 1

§ controlled entity (or subsidiary) 2 etc.]

Department Head or in accordance with a  
resolution of the Governing Board of the  
Statutory Body

(Sign and Date)

Department or Statutory Body Contact Officer

(Position and contact details)

---

## Annexe E

### Internal Audit and Risk Management Statement Template (Annual Report Disclosure)

Treasury Circular NSW TC 09/08 August 2009 requires the department head or governing board of the statutory body to report compliance with the 'core requirements' set out in the Policy annually.

The department head or governing board of the statutory body must use the relevant Internal Audit and Risk Management Statement Template (either Template E1 or E2) to make a declaration in the Annual Report that for the relevant reporting period the department or statutory body is compliant with the 'core requirements'.

#### Meaning of Compliant

'Compliant' means that for *each* core requirement *either* the department or statutory body has the core requirement 'in place' (for the financial year ending on or after 30 June 2010) or 'in operation' (for financial years ending on or after 30 June 2011) *or* the department or statutory body has a determination from the Portfolio Minister that the circumstances for an exception to the core requirement exist in the department or statutory body for the relevant reporting period.

#### Additional Disclosures

Consistent with better practice corporate governance disclosures (e.g. ASX *Corporate Governance Principles*), the department head or governing board of the statutory body may wish to modify the Internal Audit and Risk Management Statement by providing *additional* commentary on internal audit and risk management processes operating in the department or statutory body, e.g. high level commentary on the role, attendance and activities of the Audit and Risk Committee; the activities of the internal audit function; and the operation of risk management policies.

#### Reporting for Controlled Entities

Where a department or statutory body has '*control*' of an entity (or subsidiary), as defined in the Australian Accounting Standards, the parent department or statutory body should consider the impact of the controlled entity (or subsidiary) when making the declaration. The parent entity may elect to include a controlled entity (or subsidiary) in the declaration. Where a parent entity elects to do so, it should declare which controlled entities (or subsidiaries) on behalf of which the attestation is made. Where a controlled entity (or subsidiary) is scheduled under annual reporting legislation to prepare an annual report, the controlled entity (or subsidiary) must make its own declaration.

#### Presentation in Annual Report

In terms of presentation within the Annual Report, the department head or governing board of the statutory body must ensure that the Internal Audit and Risk Management Statement is co-located in the Annual Report with the existing requirement to disclose 'risk management and insurance activities'.

Template E1: No Exceptions

Internal Audit and Risk Management Statement for the  
200X-201X Financial Year for [department or statutory  
body]

*In the case of compliance with no exceptions use the following:*

I, [department head or governing board of the statutory body] am of the opinion that the [department or statutory body] has an internal audit and risk management processes in place that are, in all material respects, compliant with the core requirements set out in Treasury Circular NSW TC 09/08 *Internal Audit and Risk Management Policy*.

I, [department head or governing board of the statutory body] am of the opinion that the Audit and Risk Committee for [department or statutory body] is constituted and operates in accordance with the independence and governance requirements of Treasury Circular NSW TC 09-0. The Chair and Members of the Audit and Risk Committee are:

- § independent Chair (term of appointment)
- § independent Member 1 (term of appointment) etc.
- § non-independent Member 1 (term of appointment) etc.

[Where a department or statutory body has 'control' of an entity (or subsidiary), as defined in the Australian Accounting Standards, and the department or statutory body elects to include a controlled entity (or subsidiary) in the Statement, use the following wording to declare each of the controlled entities (or subsidiaries) on behalf of which the attestation statement is made:

I, [department head or governing board of the statutory body] declare that this Internal Audit and Risk Management Statement is made on behalf of the following controlled entities (or subsidiaries):

- § controlled entity (or subsidiary) 1
- § controlled entity (or subsidiary) 2 etc.]

These processes provide a level of assurance that enables the senior management of [department or statutory body] to understand, manage and satisfactorily control risk exposures.

Department Head or in accordance with a  
resolution of the Governing Board of the  
Statutory Body

(Sign and Date)

---

Template E2: Exceptions

Internal Audit and Risk Management Statement for the 200X-201X Financial Year for [department or statutory body]

In the case of compliance with exceptions use the following:

I, [department head or governing board of the statutory body] am of the opinion that the [department or statutory body] has an internal audit and risk management processes in place that are, excluding the exceptions described below, compliant with the core requirements set out in Treasury Circular NSW TC 09/08 *Internal Audit and Risk Management Policy*.

I, [department head or governing board of the statutory body] am of the opinion that the internal audit and risk management processes for [department or statutory body] depart from the following core requirements set out in Treasury Circular NSW TC 09/08 and that (a) the circumstances giving rise to these departures have been determined by the Portfolio Minister and (b) the [department or statutory body] has implemented [or is implementing] the following practicable alternative measures that will achieve a level of assurance equivalent to the requirement:

Ministerially Determined Departure	Reason for Departure and Description of Practicable Alternative Measures Implemented
<ul style="list-style-type: none"> <li>• Core Requirement X</li> </ul>	<ul style="list-style-type: none"> <li>• Brief description of circumstances giving rise to departure(s)</li> <li>• Brief description of the alternative measures implemented / being implemented to achieve equivalent level of assurance</li> </ul>

I, [department head or governing board of the statutory body] am of the opinion that the Audit and Risk Committee [or shared service /policy cluster equivalent] for [department or statutory body] is constituted and operate[s] in accordance with the independence and governance requirements of Treasury Circular NSW TC 09/08. The Chair and Members of the Audit and Risk Committee are:

- § independent Chair (term of appointment)
- § independent Member 1 (term of appointment) etc.
- § non-independent Member 1 (term of appointment) etc.

[Where a department or statutory body has ‘control’ of an entity (or subsidiary), as defined in the Australian Accounting Standards, and the department or statutory body elects to include a controlled entity (or subsidiary) in the Statement, use the following wording to declare each of the controlled entities (or subsidiaries) on behalf of which the attestation statement is made:

I, [department head or governing board of the statutory body] declare that this Internal Audit and Risk Management Statement is made on behalf of the following controlled entities (or subsidiaries):

- § controlled entity (or subsidiary) 1
- § controlled entity (or subsidiary) 2 etc.]

These processes, including the practicable alternative measures [being] implemented, provide a level of assurance that enables [will enable] the senior management of [department or statutory body] to understand, manage and satisfactorily control risk exposures.

Department Head or in accordance with a  
resolution of the Governing Board of the  
Statutory Body

(Sign and Date)

---