NSW GOVERNMENT | Treasury

December 2020

TPP

20-08

Policy and Guidelines Paper

Internal Audit and Risk Management Policy for the General Government Sector

Preface

The *Internal Audit and Risk Management Policy for the General Government Sector* (Policy) is a mandatory policy which has been prepared by NSW Treasury (Treasury) to assist agencies in fulfilling their legislative obligations under the *Government Sector Finance Act 2018* (GSF Act) by outlining minimum standards for risk management, internal audit and Audit and Risk Committees (ARCs). The GSF Act strengthens accountability, transparency, performance and innovation in the New South Wales Government. It sets out the key roles and responsibilities of Accountable Authorities for the financial and performance management their agencies.

Section 3.6 of the GSF Act requires the Accountable Authority of a GSF agency (generally the Secretary or agency head) **"to establish, maintain and keep under review effective systems for risk management, internal control and assurance (including by means of internal audits) that are appropriate systems for the agency".** The Policy establishes an overarching framework and the minimum standards for agencies to meet their legislated risk management, internal control and assurance requirements.

The Policy extends further than simply requiring agency compliance. It promotes the use of best practice standards and frameworks, and the tailoring of these frameworks for agencies to implement, develop, enhance and manage. The Core Requirements concerning risk management are founded on Australian Standard *AS ISO 31000:2018 Risk management – Guidelines*. The Core Requirements relating to an agency's internal audit function are founded on the Institute of Internal Auditors (IIA) *International Standards for the Professional Practice of Internal Auditing*.

The Policy supersedes the *Internal Audit and Risk Management Policy for the NSW Public Sector* (TPP15-03), *Guidance on Shared Arrangements and Subcommittees for Audit and Risk Committees* (TPP16-02) and *Small Agency Exemption to TPP15-03 - Internal Audit and Risk Management Policy for the NSW Public Sector* (TC18-16). In doing so, the Policy:

- articulates clear principles and specific Core Requirements that align with the GSF Act and the international standards as updated;
- clarifies roles and responsibilities across risk management and internal audit;
- recognises the diversity of the General Government Sector by providing flexibility for agencies to implement and manage their governance arrangements including provisions for shared arrangements;
- promotes efficient and effective oversight arrangements; and
- streamlines attestation requirements.

The Policy should be read alongside the other Policy and Guideline papers that apply to internal audit and risk management, including the *Risk Management Toolkit for the NSW Public Sector* (TPP12-03).

Acknowledgement of Country

Treasury acknowledges that Aboriginal and Torres Strait Islander peoples are the First Peoples and Traditional Custodians of Australia, and recognises their continued custodianship of Country - land, seas and skies. We acknowledge the diversity of First Nations cultures, histories and peoples, recognise their enduring connection to our State, and we pay our deepest respects to Elders past, present and emerging.

Michael Pratt AM
Secretary
NSW Treasury
December 2020

Note
General inquiries concerning this document should be initially directed to:
Director, Financial Management Policy, Treasury (Tel: 9228 5233) and/or finpol@treasury.nsw.gov.au
This publication can be accessed from the Treasury's website http://www.treasury.nsw.gov.au/.

Revision history				
Document version number	**Approval Date**	**Author**	**Approver**	**Description**
1.1	January2022	C Curtin – AD FMP	S Waters – CFOO	Minor revisions: • Repoint Annexure J to GSF Regulation schedules following repeal of the PFAA schedules • Clarify wording of instructions for attestations and exemption requests that hard copies are not required. • Remove reference to archived DPC circular C2009-13
1.2	August 2023	N Hulme – FMP	J Vandenbroek – D FMLPA	Minor Revisions • Removal of Annexure J reflecting a change in the GSF Regulation schedule 2 Removal of references to Annexure J

Contents

Executive Summary

The *Internal Audit and Risk Management Policy for the General Government Sector* (Policy) is issued as a mandatory policy to assist the Accountable Authority of agencies to comply with their legislative obligations under Section 3.6 of the GSF Act by outlining minimum standards for risk management, internal audit and Audit and Risk Committees (ARCs).

This Policy applies to agencies listed in Schedule 2 of the GSF Regulations excluding State Owned Corporations, universities and controlled entities of Universities. The legislative obligations for Accountable Authorities under Section 3.6 of the GSF Act include a requirement "to establish, maintain and keep under review appropriate and effective systems for risk management, internal control and assurance". To support the implementation of these systems in an efficient and effective manner, Accountable Authorities may form Shared Arrangements between a group of agencies within a Cluster, so long as certain requirements are met (refer to the Shared Arrangements section for further details).

In addition, the Policy seeks to strengthen internal audit, risk management and governance practices across the government sector by promoting the use of best practice standards and frameworks, which Accountable Authorities can implement and further develop. This is achieved through adopting the three Principles listed below that describe the outcomes sought from effectively implementing a risk management framework, an internal audit function and an ARC. These Principles are underpinned by the seven Core Requirements, which are preconditions for the Principles that provide the foundation of the Policy.

The Principles and Core Requirements are:

<table>
<tr><th colspan="2">1. Risk Management Framework</th></tr>
<tr><td rowspan="2">Principle 1:
Effective risk management arrangements should support the agency in achieving its objectives by systematically identifying and managing risks to:
increase the likelihood and impact of positive events
mitigate the likelihood and impact of negative events.</td><td>Core Requirement 1.1
The Accountable Authority shall accept ultimate responsibility and accountability for risk management in the agency.</td></tr>
<tr><td>Core Requirement 1.2
The Accountable Authority shall establish and maintain a risk management framework that is appropriate for the agency. The Accountable Authority shall ensure the framework is consistent with AS ISO 31000:2018.</td></tr>
<tr><th colspan="2">2. Internal Audit Function</th></tr>
<tr><td rowspan="3">Principle 2:
An internal audit function should provide timely and useful information to management about:
the adequacy of, and compliance with, the system of internal control
whether agency results are consistent with established objectives
whether operations or programs are being carried out as planned.</td><td>Core Requirement 2.1
The Accountable Authority shall establish and maintain an internal audit function that is appropriate for the agency and fit for purpose.</td></tr>
<tr><td>Core Requirement 2.2
The Accountable Authority shall ensure that the operation of the internal audit function is consistent with the International Standards for Professional Practice for Internal Auditing.</td></tr>
<tr><td>Core Requirement 2.3
The Accountable Authority shall ensure the agency has an Internal Audit Charter that is consistent with the content of the 'model charter'.</td></tr>
</table>

3. Audit and Risk Committee	
Principle 3: An independent Audit and Risk Committee with appropriate expertise should provide relevant and timely advice to the Accountable Authority on the agency's governance, risk and control frameworks and its external accountability obligations.	**Core Requirement 3.1** The Accountable Authority shall establish and maintain efficient and effective arrangements for independent Audit and Risk Committee oversight to provide advice and guidance to the Accountable Authority on the agency's governance processes, risk management and control frameworks, and its external accountability obligations.
	Core Requirement 3.2 The Accountable Authority shall ensure the Audit and Risk Committee has a Charter that is consistent with the content of the 'model charter'.

The Policy requires each Accountable Authority to self-assess whether they have been 'compliant', 'non-compliant' or 'in transition' in relation to each of the Core Requirements and produce an Attestation Statement for the prior reporting period. Where the agency is a reporting GSF agency for the purposes of Part 7 of the GSF Act, an agency's Attestation Statement is required to be included in the agency's annual reporting information for the relevant Annual Reporting Period.

The Accountable Authority for an agency is to ensure that a copy of the agency's Attestation Statement for the previous Annual Reporting Period is separately submitted to Treasury on or before **31 October** each year. Submissions to Treasury should be emailed to finpol@treasury.nsw.gov.au and addressed to the Director, Financial Management Policy.

Attesting 'compliant' to each Core Requirement means complying with the Mandatory Requirements listed below each Core Requirement. Where the agency is non-compliant with a Core Requirement(s) or Mandatory Requirement(s) of the Policy, the Accountable Authority shall mark 'non-compliant' on their Attestation Statement next to the relevant Core Requirement(s) and explain why the agency is non-compliant. The Accountable Authority shall also apply to the agency's Responsible Minister for a Ministerial Exemption from the Core Requirement(s). This shall be made prior to the reporting period in which full compliance is unable to be achieved or as soon as circumstances arise during the reporting period that will make full compliance not possible. A copy of the Ministerial Determination shall be attached to the copy of the Attestation Statement submitted to Treasury.

An agency may mark 'in transition' on their Attestation Statement where the agency meets the requirements of a Transitional Arrangement, including during the first twelve months from the commencement date of the Policy, if the agency is new (to the agencies listed in Schedule 2 of the GSF Regulations excluding State Owned Corporations, universities and controlled entities of Universities) during the reporting period or the agency is impacted by Machinery of Government changes. Refer to the Transitional Arrangements section for further details.

Templates and model charters are provided as Annexures to the Policy. With the exception of the Ministerial Determination Template, templates and charters in the Policy shall be used and adapted to the needs and circumstances of the agency. The Ministerial Determination Template has been provided as a guide only.

The Policy will be effective from 1 January 2021.

Definitions

The following lists relevant key terms and their definitions:

Accountable Authority for an agency has the same meaning as in section 2.7(2) of the GSF Act, which is, unless otherwise specified in the GSF Act, the Secretary of the Department if the agency is a Department or the head of the agency if the agency is not a Department.

Agency means agencies listed in Schedule 2 of the GSF Regulations excluding State Owned Corporations, universities and controlled entities of Universities.

Associated agency, for the purposes of the Policy, is an agency that meets one or more of the following criteria:

- is an agency that controls (the parent agency) or is controlled by another agency (a controlled entity) which has the same meaning as section 2.2 of the GSF Act
- is an agency which shares with another agency, either:
    - operations
    - resources, or
    - projects and/or service delivery areas
- is an agency co-located within the same cluster.

Attestation Statement is an annual statement in which the Accountable Authority attests to the agency's compliance with the Core Requirements of the Policy. The statement is made using the format prescribed in the Policy (Annexure C). The Statement is published in the agency's Annual Report and a copy is submitted to Treasury on or before 31 October each year.

Audit and Risk Committee (ARC) is a committee established in accordance with the Policy to monitor, review and provide advice and guidance about the agency's governance processes, risk management and internal control frameworks and external accountability obligations.

Audit and Risk Committee Charter sets out the roles and responsibilities of the ARC with respect to monitoring, reviewing and providing advice on the agency's governance processes, risk management and control frameworks and its external accountability obligations.

Audit Office means the Audit Office of New South Wales.

Chief Audit Executive (CAE) is a person within an agency (with the exception of an approved Shared Arrangement) who heads the internal audit function and is responsible for providing strategic leadership and managing the internal audit function within the agency.

Chief Financial Officer (CFO) is the most senior position in the agency with the primary responsibility and accountability for the financial management of the agency, including the preparation of external and internal financial reports and the delivery of other financial management support functions.

Chief Risk Officer (CRO) is a person that has designated responsibility for designing the agency's risk management framework and for the oversight of activities associated with coordinating, maintaining and embedding the framework in the agency.

Cluster refers to the 'administrative arrangements that bring together a group of different legal and administrative agencies and allow similar and complementary Government services to be coordinated more effectively within the broad policy area of a particular Cluster'.[1] Clusters are not legal entities.

[1] NSW Department of Premier and Cabinet, February 2013, *NSW Public Sector Governance Framework.*

Cluster Secretary is the Secretary of the Department in a cluster.

Collaborative Shared Arrangement involves a group of agencies agreeing to establish a shared ARC to provide oversight over all the entities in the shared arrangement and may include sharing a CAE and/or internal audit functions.

Compliant means that the agency has implemented and maintained practices consistent with the Core Requirements of the Policy for the whole of the financial year.

Consolidated Fund has the same meaning as in section 1.4 of the GSF Act and section 39 of the *Constitution Act 1902,* which is all public moneys (including securities and all revenue, loans and other moneys whatsoever) collected, received or held by any person for or on behalf of the State.

Controls refers to existing processes, policies, devices, practices or other actions which maintain and/or modify risks.

Core Requirements are the seven (7) requirements stated in this Policy.

Department, unless otherwise specified, means a person, group of persons or body specified in Schedule 1, Part 1 of the *Government Sector Employment Act 2013.*

General Government Sector has the same meaning as in section 1.4 of the GSF Act and includes NSW government agencies.

Government officer of a GSF agency has the same meaning as in section 2.9 of the *GSF* Act. This includes persons who are the head of, or are employed in or by, a GSF agency and statutory officers.

In transition is where the agency is in the process of transitioning its arrangements to meet requirements in the Policy or is impacted by Machinery of Government changes for which transitional arrangements have been provided.

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

Internal Audit Charter sets out the role, responsibilities, authorisation, activities and reporting relationships of the Internal Audit function within the agency.

Mandatory Requirements are the points listed below each of the Core Requirements and are required to be followed by the Accountable Authority for an agency in order to implement the Core Requirements, with the exception of Practice Notes.

New agencies are agencies that are newly added to agencies listed in Schedule 2 of the GSF Regulations during the reporting period excluding State Owned Corporations, universities and controlled entities of Universities.

Non-compliant means the agency has not been compliant with one or more Core Requirements or Mandatory Requirements of the Policy for the whole or part of the financial year.

Performance management framework refers to a framework designed to ensure that an agency's objectives are being efficiently and effectively achieved.

[2] The Institute of Internal Auditors, *International Professional Practices Framework*, 2017.

Practice Notes are best practice recommendations or clarifications about audit and risk practice included in marked boxes to support the Core Requirements of the Policy. Practice notes are intended as guidance only and do not form part of the Mandatory Requirements of the Policy.

Prequalification Scheme means the Prequalification Scheme: Audit and Risk Committees Independent Chairs and Members.[3]

Principal Department Led Shared Arrangement involves the cluster Department ARC overseeing additional agencies within its cluster and may include the sharing of a CAE and/or Internal Audit functions.

Reporting period has the same meaning as *Annual Reporting Period* in section 2.10 of the GSF Act. This is the period of 12 months commencing on 1 July in any year or, if a different period is specified as the agency's financial year by its constituent Act, that specified period.

Responsible Minister has the same meaning as in section 2.6(1) of the GSF Act.

Risk[4] is the effect of uncertainty on objectives. (Note: effect is a deviation from the expected and may be positive and/or negative).

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation.

Risk management refers to the coordinated activities to direct and control an agency with regards to risk.

Risk management framework refers to the set of components for integrating, designing, implementing, evaluating and improving risk management throughout an agency.

Risk management process is the systematic application of policies, procedures and practices to the tasks of communication, consultation, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risk.

Risk management plans identify the strategy, activities, resources, responsibilities and timeframes for implementing and maintaining risk management in an agency.

Risk treatment is a process to modify risk.

Shared Arrangements support agencies to establish efficient and effective oversight arrangements in terms of assurance and independent advice requirements while minimising the administration, financial costs and resource implications. The elements that can be shared include a Chief Audit Executive, and/or an Internal Audit Function and/or an ARC. A Shared Arrangement may take the form of a Principal Department Led Shared Arrangement or a Collaborative Shared Arrangement.

Special Office is an agency which requires independent ARC assurance arrangements due to the risk profile and/or functions of the agency. These are the agencies listed as 'separate agencies' in Schedule 1 – Part 3 of the *Government Sector Employment Act 2013* and listed as a 'Separate GSF agency' in section 2.5(1) of the GSF Act.

Treasury Attestation Statement Template is the template in Annexure C of this Policy.

---

[3] Prequalification Scheme: Audit and Risk Committee Independent Chairs and Members – Conditions – December 2020 and Prequalification Scheme: Audit and Risk Committee Independent Chairs and Members – Guidelines – December 2020.

[4] Except where specifically noted, the Policy adopts the definitions in AS ISO: Guide 31000:2018 Risk Management.

Part A: Internal Audit and Risk Management Policy

Background

The *Internal Audit and Risk Management Policy for the NSW Public Sector* (TPP09-05) was first issued as a Treasurer's Direction in 2009 and subsequently re-issued in 2015 as the *Internal Audit and Risk Management Policy for the NSW Public Sector* (TPP15-03). TPP09-05 and TPP15-03 outlined a 'better practice' approach to internal audit and risk management that drew on the standards endorsed by professional associations and the practice of exemplar agencies in the public and private sectors.

The *Internal Audit and Risk Management Policy for the General Government Sector* (the Policy) is a mandatory policy that supersedes TPP15-03 but retains the same broad policy direction. The Policy also supersedes the *Guidance on Shared Arrangements and Subcommittees for Audit and Risk Committees* (TPP16-02) and incorporates guidance to enable agencies to form Shared Arrangements and to form Subcommittees of ARCs.

The main areas of amendment to TPP15-03 (and TPP16-02) reflected in this Policy, include:

- Alignment with the new GSF Act, including terminology changes:
    - *agency head* changed to *Accountable Authority*
    - *Department* and *agency* are now both referred to as *GSF agency*
    - *NSW Public Sector* changed to *General Government Sector*
    - *Officer of an authority* and *accounting officer* changed to *government officer of a GSF agency*, and
    - *Portfolio Minister* changed to *Responsible Minister*
- An update of the Policy and Core Requirement 1.2 to reflect the new international standard *AS ISO 31000: 2018 Risk management – Guidelines*
- References to updated Treasury Policies (throughout)
- Addition of the Small Agency Exemption (refer to Annexure E for more details)
- Updating the transitional arrangements, including for Machinery of Government changes (pages 16-17)
- An update of Core Requirement 3.1 to combine previous Core Requirements 3.1 and 3.2 of TPP15-03
- Additional guidance on administrative and functional reporting lines for CAEs (Pages 28-29, Core requirement 2.1.14)
- Increasing the flexibility for agencies to form Shared Arrangements (Pages 12-14, Core requirement 3.1.2-3.1.4 and Annexure G)
- Updating ARC responsibilities in the ARC charters (Annexure B, H and I)
- Consolidating the guidance on Subcommittees of ARCs (Core requirement 3.1.23 - 3.1.31)
- Additional guidance on emerging risks and promoting a positive risk culture (Core requirement 1.2.6 and 1.2.11 to 1.2.13).

Application of the Policy

The Policy is issued as a mandatory policy to assist agencies to comply with their obligations under Section 3.6 of the GSF Act.

This Policy applies to the GSF agencies listed in Schedule 2 of the *Government Sector Finance Regulations 2018* (GSF Regulations) with the exception of State Owned Corporations and Universities. **This Policy also applies to any agency listed in Schedule 2 of the GSF Regulations after the commencement of this Policy excluding SOCs, universities and controlled entities of Universities.** If there is a change in the name of a listed GSF agency and the purpose and functions of the agency remain the same, then the Policy continues to apply to this agency.

The Policy withdraws and replaces the previous *Internal Audit and Risk Management Policy for the NSW Public Sector* (TPP15-03), *Guidance on Shared Arrangements and Subcommittees for Audit and Risk Committees* (TPP16-02) and the *Small Agency Exemption to TPP15-03 - Internal Audit and Risk Management Policy for the NSW Public Sector* (TC18-16). The Policy will take effect from 1 January 2021.

The ***Accountable Authority*** may delegate any functions in the Policy to a ***government officer*** of a ***GSF agency***. However, the ultimate responsibility for meeting all requirements in the Policy remains with the Accountable Authority.

Relationship to legislation and existing policies

GSF Act requirements

The Policy supports Accountable Authorities in meeting their obligations under section 3.6 of the GSF Act including setting out how Accountable Authorities can fulfil the requirement, under section 3.6(1)(b) "to establish, maintain and keep under review effective systems for risk management, internal control and assurance (including by means of internal audits) that are appropriate for the agency".

Related Policies

The Policy should be read in conjunction with related Treasurer's Directions, circulars and policies including:

- Treasury Policy and Guidelines Papers:
  - *Risk Management Toolkit for NSW Public Sector agencies* (TPP12-03)
  - *Certifying the Effectiveness of Internal Controls Over Financial Information* (TPP17-06)
  - *Treasury Risk Maturity Assessment Tool Guidance Paper* (TPP20-06)
- Circulars and policies relating to the Prequalification Scheme: Audit and Risk Committee Independent Chairs and Members:
  - Prequalification Scheme: Audit and Risk Committee Independent Chairs and Members – Conditions – December 2020
  - Prequalification Scheme: Audit and Risk Committee Independent Chairs and Members – Guidelines – December 2020
  - Code of Conduct: Audit and Risk Committee Chairs and Members
  - Department of Premier and Cabinet Circular No. 2009-13 – Prequalification Scheme: Audit and Risk Committees May 2009.

Purpose and Principles of the Policy

The Policy supports Accountable Authorities in meeting their obligations under section 3.6(1)(b) of the GSF Act. In addition, it seeks to strengthen internal audit, risk management and governance practices across agencies. This is achieved through adopting the three Principles listed below, which describe the outcomes sought from effectively implementing a risk management framework, an internal audit function and ARC. Agencies should implement a cycle of continuous improvement whereby they can assess whether their systems, processes and procedures are consistent with the spirit of the Policy.

Principle 1

1. Effective risk management arrangements should support the agency in achieving its objectives by systematically identifying and managing risks to:

- increase the likelihood and impact of positive events
- mitigate the likelihood and impact of negative events.

Principle 2

2. An internal audit function should provide timely and useful information to management about:

- the adequacy of, and compliance with, the system of internal control
- whether agency results are consistent with established objectives
- whether operations or programs are being carried out as planned.

Principle 3

An independent Audit and Risk Committee with appropriate expertise should provide relevant and timely advice to the Accountable Authority on the agency's governance, risk and control frameworks and its external accountability obligations.

The Policy recognises that, to be effective, a governance structure will be comprised of management functions; risk, control and compliance oversight functions; and independent assurance functions. These are elements demonstrated in the IIA's **'Three Lines Model'** which individually and together, contribute to an environment of effective governance and informed decision making. The Three Lines Model is illustrated in Figure 1 below and has been adapted to include where the risk management function, internal audit function and the ARC fit within this structure.

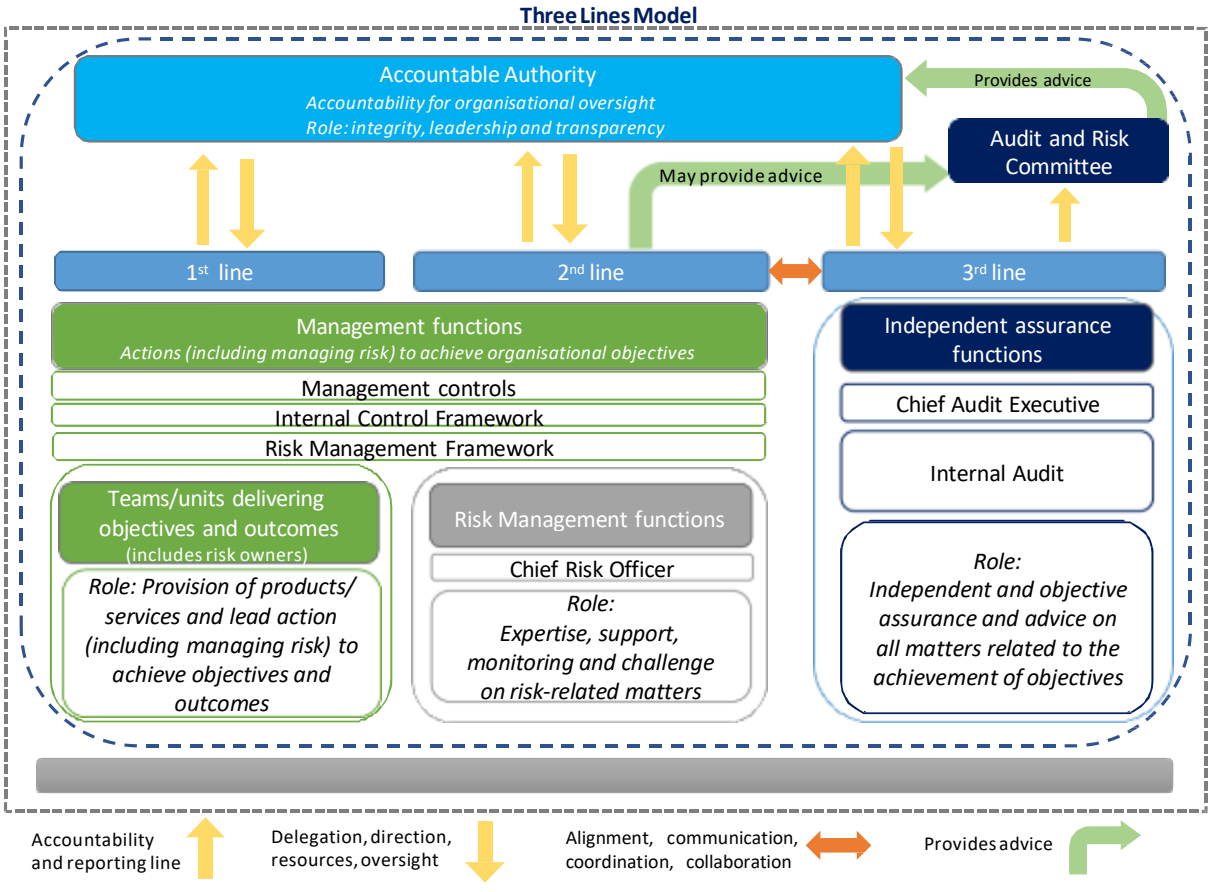


Figure 1: Context for the Internal Audit and Risk Management Policy

The Three Lines Model[5] can further be described as follows:

- The first and second line roles may be blended or separated
- First line relates to functions that deliver services, products and/or projects to achieve the agency's objectives and outcomes. Risk originates with these functions and therefore they are responsible for owning and managing risk, having in place processes to show controls are working effectively and a continual focus on risk management
- Second line relates to functions that oversee or specialise in risk management and compliance and provides support to the first line functions. It includes reviewing and monitoring the effectiveness of risk management including the first line's internal controls and activities and may include broader responsibilities including enterprise risk management
- Third line relates to functions that provide independent assurance and advice to the Accountable Authority on the adequacy and effectiveness of both first and second line governance and risk management approaches.

The ARC has an oversight role to provide advice and guidance to the Accountable Authority with input from the CAE and Internal Audit (third line). While the Chief Risk Officer and the risk management function report functionally to the Accountable Authority, they would also provide information to the ARC to support their oversight role.[6]

Risk management is an integral part of good management and leadership. Effective decision making will reflect effective risk management. Successful management of risks will increase the likelihood of an agency achieving its objectives, both in the short and longer term.

A risk management framework provides a structure that will facilitate the use of a consistent risk management process wherever decisions are being made in an agency. This includes all projects, functions and activities at all levels.

Internal audit relies on, and complements, an agency's risk management framework. The internal audit work plan should be based on an assessment of an agency's key risks and provide assurance, through independent review, that the agency controls have been designed to manage organisational risk and achieve the entity's objectives, and that these controls are operating effectively. This process of review will, in turn, identify and inform agency management of areas of new or altered risk thereby feeding back into the agency's risk management framework. Internal audit has a key advisory role to play in, among other things, providing assurance to the Accountable Authority that the design and operation of the risk management framework is effective.

The **Audit and Risk Committee** provides independent advice and guidance to the Accountable Authority by monitoring and reviewing the agency's governance processes, internal audit function, risk management and control frameworks and its external accountability obligations.

It is through these distinct yet critically interrelated components that an agency can develop an effective governance framework to underpin informed decision making and the achievement of its strategic and operational objectives.

Core Requirements of the Policy

Accountable Authorities shall comply with the following seven Core Requirements that are set out in detail in Part B of the Policy:

---

5 Adapted from: Cox, A 2017 *Whitepaper-internal audit independence arrangements*, The Institute of Internal Auditors – Australia, Sydney, NSW; The Institute of Internal Auditors – Australia, *Factsheet: '3 lines of defence' combined assurance model*, Australia, 2020; The Institute of Internal Auditors - Global, *The IIA's three lines model – an update of the three lines of defence,* July 2020.

6 As noted in 1.1.7 and 2.1.14, all agencies are encouraged to nominate a CRO. However, the role of the CRO and CAE may be carried out by the same individual, provided appropriate safeguards are implemented, refer to the practice note in 2.1.12.

1. Risk Management Framework	
Principle 1: Effective risk management arrangements should support the agency in achieving its objectives by systematically identifying and managing risks to: ▪ increase the likelihood and impact of positive events ▪ mitigate the likelihood and impact of negative events.	**Core Requirement 1.1** The Accountable Authority shall accept ultimate responsibility and accountability for risk management in the agency.
	Core Requirement 1.2 The Accountable Authority shall establish and maintain a risk management framework that is appropriate for the agency. The Accountable Authority shall ensure the framework is consistent with *AS ISO 31000:2018*.
2. Internal Audit Function	
Principle 2: An internal audit function should provide timely and useful information to management about: ▪ the adequacy of, and compliance with, the system of internal control ▪ whether agency results are consistent with established objectives ▪ whether operations or programs are being carried out as planned.	**Core Requirement 2.1** The Accountable Authority shall establish and maintain an internal audit function that is appropriate for the agency and fit for purpose.
	Core Requirement 2.2 The Accountable Authority shall ensure the internal audit function operates consistent with the International Standards for Professional Practice for Internal Auditing.
	Core Requirement 2.3 The Accountable Authority shall ensure the agency has an Internal Audit Charter that is consistent with the content of the 'model charter'.
3. Audit and Risk Committee	
Principle 3: An independent Audit and Risk Committee with appropriate expertise should provide relevant and timely advice to the Accountable Authority on the agency's governance, risk and control frameworks and its external accountability obligations.	**Core Requirement 3.1** The Accountable Authority shall establish and maintain efficient and effective arrangements for independent Audit and Risk Committee oversight to provide advice and guidance to the Accountable Authority on the agency's governance processes, risk management and control frameworks, and its external accountability obligations.
	Core Requirement 3.2 The Accountable Authority shall ensure the Audit and Risk Committee has a Charter that is consistent with the content of the 'model charter'.

The Core Requirements are preconditions for, and support the realisation of, the Principles that provide the foundation of the Policy. The Mandatory Requirements support the implementation of the Core Requirements.

Requirements for an Attestation Statement

The Accountable Authority shall attest the agency's compliance with the Core Requirements in an Attestation Statement published in the agency's annual report, with a copy provided to Treasury on or before 31 October each year. Accountable Authorities shall use the relevant Attestation Statement template at Annexure C of the Policy.

The Accountable Authority shall self-assess and determine whether the agency has been 'compliant', 'non-compliant' or 'in transition' in relation to each of the Core Requirements for the reporting period.

Where an agency determines that it has been compliant with a Core Requirement, the Accountable Authority need only note that the agency has been 'compliant' with the relevant Core Requirement on

the Attestation Statement. Compliant means complying with the Core Requirements for the whole financial year.

Where an agency determines that it has been 'non-compliant' or 'in transition', agencies should refer to the 'Ministerial Exemption Process,' 'Transitional Arrangement' and 'Small Agency Exemption' sections below.

If an agency has entered into an approved Shared Arrangement, details of the arrangement shall be stated in the Attestation Statement, including the participating agencies, resources shared and type of Shared Arrangement (e.g. CAE and/or Internal Audit Function and/or ARC and/or other resources).

The Accountable Authority shall:

a) Publish the Attestation Statement in the agency's Annual Report (provided the agency is a reporting GSF agency for the purposes of Part 7 of the *GSF* Act)

b) Submit a copy of the Attestation Statement **separately** to Treasury on or before 31 October each year. For any non-compliance with Core Requirements, agencies will be required to also submit a copy of the relevant Responsible Minister's approved Ministerial Exemption. Submissions to Treasury should be emailed to finpol@treasury.nsw.gov.au and addressed to the Director, Financial Management Policy.

Variations that apply to the Policy

As there are varying sizes and complexities of agencies across the general government sector, the Policy allows for certain variations to support its efficient and effective implementation. Refer to the below variations to determine if they are applicable to your agency.

Variations	Page references
i) Shared Arrangements A. Shared Audit and Risk Committee B. Shared Chief Audit Executive C. Shared Internal Audit Function	Pages 12-14 Core requirement 3.1.2-3.1.4 Annexure G
ii) Ministerial Exemption Process Ministerial exemption to one or more of the Core Requirements for up to two reporting periods	Pages 14-15 Annexure D
iii) Small Agency Exemption Ongoing exemption to comply with one or more of the Core Requirements until any of the listed circumstances occurs.	Pages 15-16 Annexure E
iv) Transitional Arrangements 12-month transitional period if the agency is in one or more of the following circumstances: ▪ during the first twelve months from the commencement date of the Policy ▪ new agency required to comply with the Core Requirement(s) of the Policy; or ▪ impacted by Machinery of Government (MoG) changes	Pages 16-17

i) Shared Arrangements

The aim of Shared Arrangements is to ensure that the compliance cost of implementing the Core Requirements for agencies is proportionate to their benefit and commensurate with their risk profile. Shared Arrangements may be formed between agencies to support Accountable Authorities with implementing the Core Requirements in an efficient and effective manner.

The resources that may be shared to achieve efficiencies include sharing the cost of the:

A. ARC (engaging independent ARC members and Chair and secretariat services), and/or
B. CAE, and/or
C. Internal Audit Function.

Regardless of the form of a Shared Arrangement, approval by the Cluster Secretary of Shared Arrangements does not diminish each Accountable Authority's responsibility to meet their obligations under s 3.6 of the GSF Act. This includes ensuring efficient and effective independent advice and oversight continues to be provided to each Accountable Authority and CAEs and/or Internal Audit Functions have the capacity to operate effectively.

The below and Annexure G explain variations to Core Requirements 2.1, 3.1 and 3.2 for Shared Arrangements.

Requirements of a Shared Arrangement

Accountable Authorities may enter their agency into a shared arrangement if the:

- Requirements of a Principal Department Led or Collaborative Shared ARC are met, if applicable (refer to Annexure G - A. Shared Audit and Risk Committees), and/or
- Requirements of sharing a CAE and/or Internal Audit function are met, if applicable (refer to Annexure G - B. Shared CAE and internal audit functions), and
- Shared Arrangements Agreement is signed by all Accountable Authorities in the Shared Arrangement (refer to Annexure G – Shared Arrangement Agreement), and
- Cluster Secretary approves the Shared Arrangement.

Annexure G provides further information on the requirements to form a Shared Arrangement.

A. Shared Audit and Risk Committees

Under Core Requirement 3.1, the Accountable Authority of each agency is responsible for establishing efficient and effective arrangements for ARC oversight to oversee and monitor governance, risk and control issues affecting the operations of the agency. A shared ARC (Principal Department Led or Collaborative) can be an efficient and effective means of providing ARC oversight for a number of agencies. At a cluster level, a shared ARC can leverage cost efficiencies in operating ARCs, group agencies with common functions to share the specialist skills of ARC members and improve communication between entities within the cluster.

For each cluster, the Secretary of the Department in that cluster (Cluster Secretary) can support this by ensuring efficient and effective oversight arrangements are established within their cluster and sufficient advice and guidance is provided to each agency's Accountable Authority.

Regardless of the form of arrangement, a shared ARC will operate as an individual ARC for each separate agency. This requires members of the ARC to liaise with the respective Accountable Authority, ensure separate records and confidentiality are maintained and provide independent advice and oversight for each participating agency.

Refer to Annexure G for further details on shared ARCs including adapting the Core Requirements for a Shared Arrangement.

B. Shared CAE and internal audit functions

The decision to share a CAE and/or Internal Audit Function is independent from the decision to share an ARC. There may be some instances where it is not appropriate for an agency to share a CAE and/or Internal Audit Function but still be able to enter a Shared Arrangement for an ARC (subject to the requirements relating to Shared ARCs in Annexure G being met).
When reviewing a proposal to share a CAE and/or Internal Audit Function, the Cluster Secretary is to consider the likely demands on the CAE and/or Internal Audit Function as a result of the Shared Arrangement. This should include the CAE and/or Internal Audit Function having the capacity to understand the different business activities of multiple agencies and manage the larger workload. The Cluster Secretary may consult with applicable ARCs on this matter.

Refer to Annexure G for further details on the requirements to share a CAE and/or internal audit functions.

Application process for a Shared Arrangement

It is the responsibility of the Accountable Authority for each agency to decide the appropriate assurance arrangements for their agency, including whether to enter a shared arrangement.

Where the Accountable Authorities in a cluster:

- have identified an opportunity to enter into a shared arrangement,
- are satisfied that their agencies meet the 'Requirements of a Shared Arrangement' as set out in Annexure G, and
- have agreed to pursue a shared arrangement (i.e. Principal Department Led or Collaborative ARC and/or the sharing of a CAE and/or internal audit functions),

they shall jointly address a letter seeking approval for a shared arrangement to their Cluster Secretary.

The letter should:

- identify the agencies proposing to enter into a shared arrangement
- include a brief description of the proposed arrangement including resources to be shared (ARC and/or CAE and/or internal audit functions) and how specific Core Requirements will be varied under equivalent alternative shared arrangements (refer to the Variations to the Core Requirements table for examples)
- address how each of the Requirements of a Principal Department Led or Collaborative shared ARC arrangement are met
- address, if applicable, how each of the requirements of sharing a CAE and/or Internal Audit function are met and details of which agency will provide the shared CAE and/or internal audit function
- include the proposed Shared Arrangement Agreement to be signed by the Accountable Authorities of all participating agencies
- include the Shared Audit and Risk Committee Charter
- include, if applicable, the Internal Audit Charter.

Once approved, a copy of the letter, accompanying documents and approval documentation shall be provided to Treasury as a record of approved Shared Arrangements.

Documents to be provided to Treasury should be emailed to finpol@treasury.nsw.gov.au, and addressed to the Director, Financial Management Policy.

The above application process is repeated if there is a change to a previously approved shared arrangement (e.g. an additional agency is added to a shared ARC).

The Cluster Secretary's approval of a shared arrangement in accordance with the above requirements, and the participating agencies' compliance with the Shared Arrangement Agreement's terms, constitutes compliance with the relevant Core Requirements in this Policy. Details of the shared arrangement shall be included in the Attestation Statement. Refer to the Requirements for an Attestation Statement section for further details.

For the avoidance of doubt, an exemption to this Policy is not required if the agency is part of a Shared Arrangement that has been approved by the Cluster Secretary. Unless provided for in this section and by an approved Shared Arrangement, all other Core Requirements in this Policy shall be followed.

ii) Ministerial Exemption Process

The Accountable Authority shall attest the agency's compliance with the Core Requirements in an Attestation Statement.

Where full compliance with a Core Requirement(s) during a reporting period is not possible and the deficiency is not covered by a transitional arrangement (refer to Transitional Arrangements below), the Accountable Authority shall apply to the agency's Responsible Minister for a Ministerial Exemption from the Core Requirement(s) in writing. This shall be made prior to the reporting period in which full compliance is unable to be achieved or as soon as circumstances arise during the reporting period that will make full compliance not possible.

Application to the Responsible Minister for a Ministerial Exemption

The Responsible Minister for an agency may exempt an agency, in writing, from compliance with one or more of the Core Requirements, but only if satisfied that the Accountable Authority's application has sufficiently addressed each of the matters listed below and the Core Requirements.

This application by the Accountable Authority shall:

- demonstrate how the requirements for a Ministerial Exemption listed below are met,
- provide the reasons why the agency cannot comply with each Core Requirement, and
- describe and demonstrate the agency's efforts to implement alternative arrangements and how these will achieve an outcome equivalent to the Core Requirement(s).

A Ministerial Determination Template is provided at Annexure D of the Policy to assist agencies making an application for a Ministerial Exemption.

Ministerial Exemption requirements

The requirements for a Ministerial Exemption are that:

- the agency cannot comply with the Core Requirements because of one or more of the following:
    - temporary extenuating circumstances, or
    - substantial structural constraints, or
    - resourcing constraints that will materially impact the agency's operating budget

and

- the agency is not able to enter into appropriate Shared Arrangements[7]

and

- current or proposed alternative arrangements will achieve outcomes equivalent to the requirement(s).

Approved Ministerial Exemptions

A Ministerial Determination in respect to approving a Ministerial Exemption will be operative for two (2) reporting periods only and, even where the circumstances for the initial Ministerial Exemption are ongoing, shall be renewed every two (2) years.

The Accountable Authority shall note on the Attestation Statement (refer to Annexure C of the Policy) that an agency has been 'non-compliant' with a Core Requirement(s) and provide an explanation of the departure from the Policy. The Accountable Authority shall also indicate that a Ministerial Exemption from a Core Requirement(s) has been determined by the Responsible Minister.

In such cases, the Accountable Authority shall retain documentary evidence of the Responsible Minister's Determination (refer to the template in Annexure D) and submit this material to Treasury as an attachment to the Attestation Statement on or before 31 October.

Any approved Ministerial Exemptions granted by prior to the commencement of the Policy will continue to remain in force under the provisions of this Policy, until the expiration of the Ministerial Determination.

iii) Small Agency Exemption

The Accountable Authority of an agency may apply to Treasury for an ongoing Small Agency Exemption from the requirement to:

a. comply with one or more of the Core Requirements;
b. attest compliance, and/or
c. include the Attestation Statement in the agency's annual reporting information

if:

i. the agency satisfies each of the eligibility criteria below, and
ii. the Responsible Minister of the agency approves the application for an exemption, and
iii. Treasury, as delegated authority of the Treasurer, provides final approval.

i. Eligibility criteria

Agencies may apply to Treasury for a Small Agency Exemption if the agency meets all of the following criteria:

- does not collect taxes on behalf of the NSW Government
- does not receive a direct appropriation from the Consolidated Fund
- is not controlled by an agency required to comply with the Policy
- is an agency considered by Treasury to be immaterial
- does not have annual revenue or expenditure exceeding $15m
- does not have financial assets exceeding $15m
- does not have liabilities exceeding $15m (unless the nature of the liabilities are such that complying with the Policy is deemed not to be required)
- is not a fund manager responsible for the administration and/or management of public monies
- has a risk register that indicates that their risks have been properly identified and that proper measures are in place and being monitored to manage those risks, and
- does not have a risk profile that would warrant full compliance with the Core Requirement(s).

[7] Consistent with the Shared Arrangements section and Annexure G.

ii. Responsible Minister grants approval for exemption

An Accountable Authority for an agency shall seek and be granted written approval from the Responsible Minister before applying to Treasury for a Small Agency Exemption. An Accountable Authority's request to the Responsible Minister for such approval shall:

- include evidence that the agency meets all the eligibility criteria above, and
- outline the reasons the agency should be exempt from the relevant Core Requirement(s).

iii. Application to Treasury for approval of exemption

The Accountable Authority shall apply to Treasury for a Small Agency Exemption using the template in Annexure F once written approval is obtained from the Responsible Minister.

The application to Treasury shall include:

- a copy of the Responsible Minister's written approval of the agency's application for Small Agency Exemption
- written evidence demonstrating how the agency meets each of the above eligibility criteria
- a copy of the most recent annual report of the agency or the audited financial statements for the agency
- a copy of the agency's organisational risk register including a summary of major risks faced by the agency, together with risk treatment strategies adopted by the agency to manage those risks.

Exemption Review Process

Upon notification of the successful grant of a Small Agency Exemption, the exemption will remain in force until any of the following circumstances occur:

- any major changes to the agency's structure
- the agency receives a direct appropriation
- the agency's revenues include taxes
- the agency's revenues, expenses or liabilities individually increase by more than 20% from the baseline totals/balances indicated in the audited financial statements used for the purposes of assessing the application
- the agency's risk profile materially changes.

Any Small Agency Exemptions granted by Treasury prior to the commencement of the Policy will continue to remain in force under the provisions of this Policy.

The Accountable Authority for an agency with an approved Small Agency Exemption shall consider whether the agency has met any of the above circumstances as at 31 March annually and notify Treasury of any changes no later than 30 April. Upon receipt of such a notification, the information will be reviewed and the agency will be advised as to whether the Small Agency Exemption remains in force.

Refer to Annexure E for further guidance on applying for a Small Agency Exemption.

iv) Transitional Arrangements

Where an agency is not fully compliant with a Core Requirement(s) during the reporting period, the Accountable Authority is permitted to record 'in transition' next to the relevant Core Requirement(s) in the agency's Attestation Statement (refer to Annexure C), if the following conditions are met:

- the agency is in one or more of the following circumstances:

a) it is during the first twelve months from the commencement date of the Policy; or

b) it is a new agency required to comply with the Core Requirement(s) of the Policy; or

c) it is impacted by Machinery of Government (MoG) changes.

and

- the Accountable Authority of the agency takes steps to achieve full compliance with the Core Requirement(s) within the 12-month transitional period

and

- the Accountable Authority details how the agency plans to achieve full compliance with the relevant Core Requirement(s) within the 12-month transition period in the space provided on the Attestation Statement.

Agencies taking advantage of transitional arrangements are not required to apply to the agency's Responsible Minister for a Ministerial Exemption from the Core Requirement(s) for that reporting period.

Circumstances when agencies are 'in transition'

a) During the **first twelve months** from the commencement date of the Policy, all applicable agencies will be provided with a transitional period to provide reasonable time for the implementation of arrangements for compliance with the Core Requirements of the Policy. Agencies are expected to take steps to comply with all the Core Requirements of the Policy within the twelve month period.[8]

b) **New agencies** are agencies that are newly listed in Schedule 2 of the GSF Regulations during the reporting period, excluding State Owned Corporations, universities and controlled entities of Universities. New agencies are expected to take steps to comply with all the Core Requirements of the Policy during the first twelve months from the date of inclusion.

c) There is a **Machinery of Government (MoG) change** during the financial year which results in an Accountable Authority of an agency being unable to comply with a Core Requirement(s). Impacted agencies are expected to take steps to achieve full compliance within twelve months of the MoG change. A MoG change may include (but is not necessarily limited to):
   - a change in the number of clusters
   - movement of an agency to another cluster
   - movement of a substantial function within an agency to another agency
   - significant structural change within the agency.

Monitoring of Policy Compliance

The Policy requires that Accountable Authorities publish an Attestation Statement in the Annual Report each year attesting compliance with the Core Requirements.

Periodically, the Auditor-General may undertake assurance activities in relation to the Policy. This includes monitoring the sector's compliance with the Core Requirements outlined in the Policy by conducting compliance audits.

Treasury will, on a periodic basis and at least once each five (5) years, 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. Updates to the Policy that take place between formal reviews may be made as version updates and agencies notified accordingly.

[8] Agencies shall remain compliant with the existing requirements in TPP15-03 during the first twelve months from the commencement of the Policy. Where agencies are compliant with TPP15-03 but not the Policy during the first twelve months, agencies may mark 'in transition'. Where agencies are not compliant with either TPP15-03 or the Policy during the first twelve months, agencies must mark 'not compliant' on their Attestation Statement and obtain a Ministerial Exemption.

Part B: Instructions for implementing the Core Requirements

1. Risk Management Framework

Principle 1:

Effective risk management arrangements should support the agency in achieving its objectives by systematically identifying and managing risks to:

- increase the likelihood and impact of positive events
- mitigate the likelihood and impact of negative events.

Core Requirements 1.1 – The Accountable Authority shall accept ultimate responsibility and accountability for risk management in the agency.

Definition of Risk

1.1.1 Except where noted, the Policy adopts the definitions in the *AS ISO 31000:2018 Risk management – Guidelines* including:

Risk being the effect of uncertainty on objectives, noting that effect is a deviation from the expected and may be positive and/or negative.

1.1.2 In addition, for the purposes of the Policy:

Risk management plans identify the strategy, activities, resources, responsibilities and timeframes for implementing and maintaining risk management in an agency.

A ***Chief Risk Officer (CRO)*** is a person that has designated responsibility for designing the agency's risk management framework and for the oversight of activities associated with coordinating, maintaining and embedding the framework in an agency.

Risk Management Roles and Responsibilities

1.1.3 The Accountable Authority has ultimate responsibility and accountability for risk management in the agency. The Accountable Authority's risk management related responsibilities also include promoting a positive risk culture, determining and articulating the level of risk the agency is willing to accept or tolerate, approving the agency's risk management policy and plans and ensuring these are communicated, implemented and kept current.

1.1.4 The Accountable Authority is responsible for ensuring that managers and decision makers at all levels in the agency understand that they are accountable for managing risk within their sphere of authority and in relation to the decisions they take.

1.1.5 The Accountable Authority is responsible for ensuring that all staff (permanent, temporary or contract) are aware they are accountable for managing risk in their day to day roles, including carrying out their roles in accordance with policies and procedures, identifying risks and inefficient or ineffective controls and reporting these to the appropriate level of management.

1.1.6 Internal audit is responsible for providing assurance to the Accountable Authority and the ARC on the effectiveness of the risk management framework including the design and operational effectiveness of internal controls.

1.1.7 The roles and responsibilities of the ARC with respect to risk management are outlined in the Model Audit and Risk Committee Charter at Annexure B.

Practice Note - Appointing a CRO

All agencies are encouraged to nominate an appropriately skilled CRO who is responsible for the oversight and promotion of risk management within the agency, designing the agency's risk management framework and for the oversight of activities associated with coordinating, maintaining and embedding the framework in the agency. The CRO should also be a member of the agency's senior management team where possible.

Core Requirements 1.2 – The Accountable Authority shall establish and maintain a risk management framework that is appropriate for the agency. The Accountable Authority shall ensure the framework is consistent with *AS ISO 31000:2018*.

Risk Management Standard

1.2.1 The Government has approved the application of the current Australian Standards (AS) on risk management in the government sector. The current standard is *AS ISO 31000:2018 Risk management - Guidelines*. This standard sets out a generic process for managing any form of risk in a systematic, transparent and credible manner and within any scope and context.[9]

1.2.2 The Accountable Authority shall establish and maintain a risk management framework that is appropriate, fit for purpose, tailored to the needs of the agency and consistent with *AS ISO 31000:2018*.

Practice Note - Principles-based guidance

AS ISO 31000:2018 consists of a set of principles, a framework and a process for managing risks. Managing risk assists agencies in setting strategy, achieving agency objectives and making informed decisions. It is not a compliance standard, but instead provides principles-based guidance on best practice.

1.2.3 *AS ISO 31000:2018* describes the principles that provide the foundation for managing risk and a framework to assist agencies in integrating risk management into the governance of the agency.

AS ISO 31000:2018 identifies eight principles that are the foundation for risk management to be effective. As reflected in Figure 2, risk management should:

- be integrated with organisation processes
- be structured and comprehensive
- be customised – the framework and process are customised and proportionate to the agency's external and internal context related to its objectives
- be inclusive – appropriate and timely involvement of stakeholders enables their knowledge, views and perceptions to be considered, resulting in improved awareness and informed risk management
- be dynamic – effective risk management anticipates, detects, acknowledges and responds to internal and external changes in a timely manner

[9] International Organization for Standardisation (ISO) 2018, *ISO 31000: 2018 Risk management – Guidelines,* ISO, Geneva.

- be based on the best available information - inputs to risk management are based on historical and current information, future expectations and any associated limitations and uncertainties
- take human and cultural factors into account
- involve continual improvement – through learning and experience.

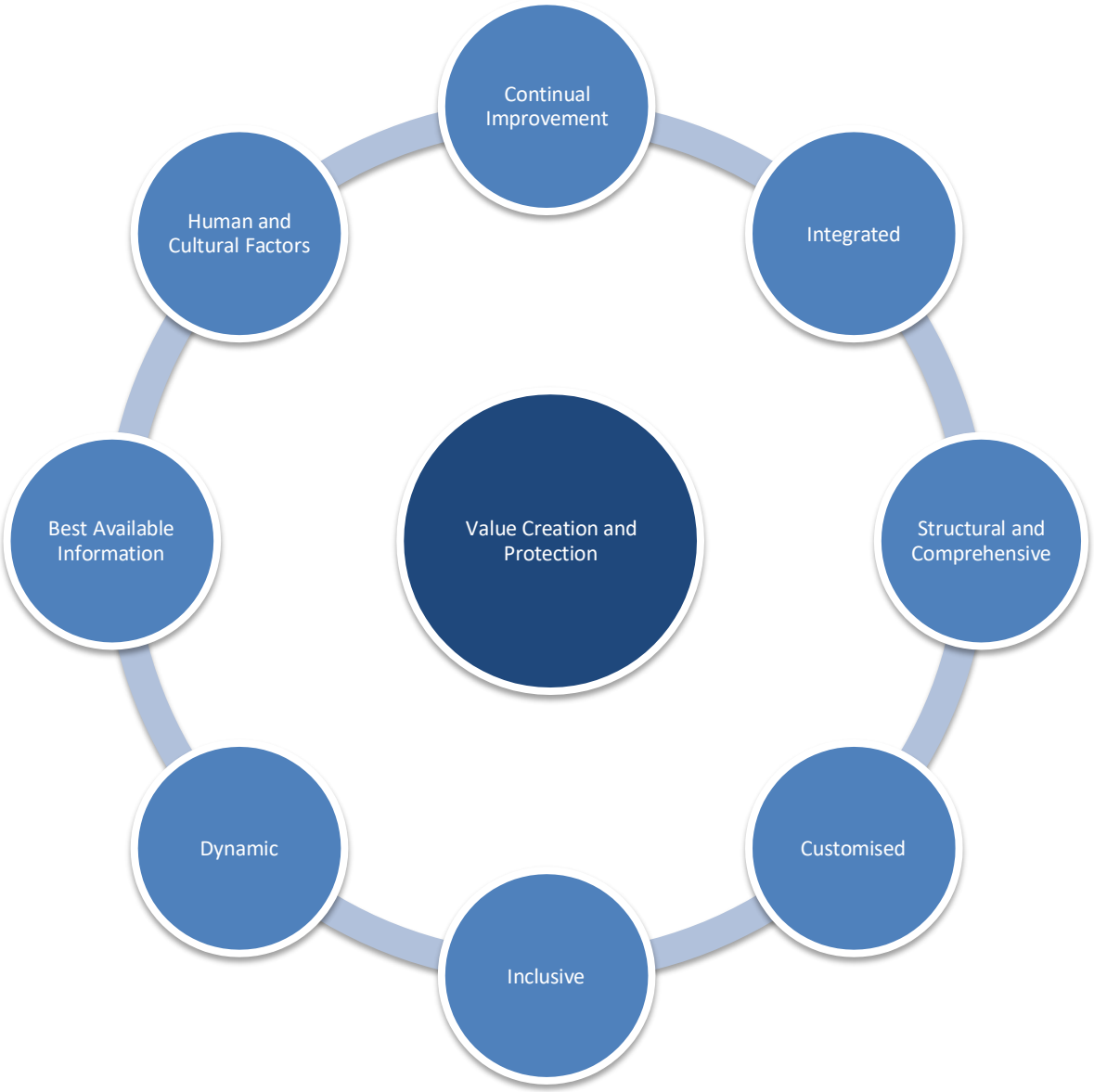


Figure 2: Key principles of risk management

1.2.4 The key elements of a risk management framework as illustrated below in Figure 3 are:

- **Leadership and Commitment** – the Accountable Authority and senior management should integrate risk management into all organisational activities and demonstrate leadership and commitment by:
  - customising and implementing all components of the framework
  - establishing a risk management policy
  - assigning authority, accountabilities and responsibilities at the appropriate level, and
  - committing resources to manage risk.
- **Integration** of risk management into an agency should be a dynamic and iterative process and should be customised to the agency's needs and culture. It should be part of and not

separate from the agency's purpose, governance, leadership, commitments, strategy, objectives and operations.

- **Design** of the framework for managing risk should be based on an understanding of the internal and external context of the agency and should:
  - demonstrate continual commitment to risk management
  - assign risk management roles, responsibilities, authorities and accountabilities
  - allocate resources
  - establish an approved approach to communication and consultation to support the framework and facilitate effective risk management.
- **Implementing a risk management framework** by developing an appropriate plan, identifying decision makers, modifying decision making processes if necessary and ensuring risk management processes and arrangements are well understood by the agency and practised.
- **Evaluation** – should periodically measure the risk management framework against its purpose, implementation plans and expected behaviours and reviewed to ensure it is fit for purpose and remains consistent with the agency's objectives.
- **Continual improvement of the framework** – continuously monitor and adapt the framework to address external and internal changes. The suitability, adequacy and effectiveness of the framework should be continuously improved to support the agency moving to a higher level of maturity in risk management.

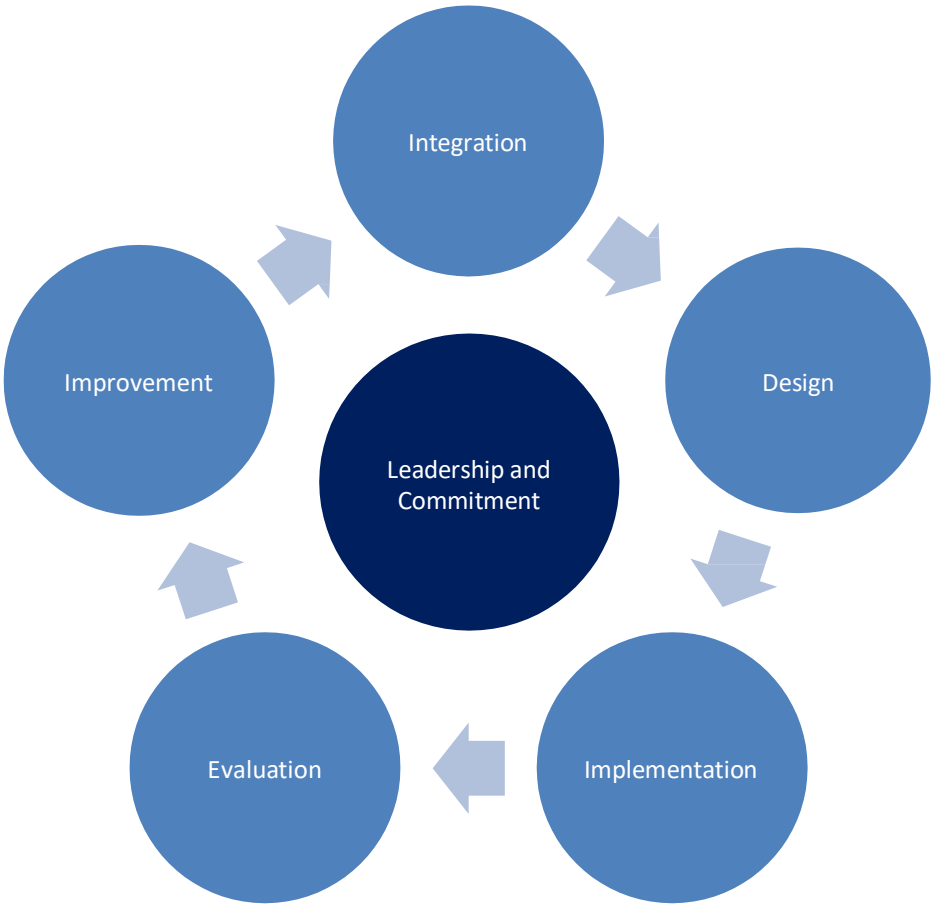


Figure 3: Key elements of a risk management framework (adapted from AS ISO31000:2018)

Practice Note - Evaluation of Risk Management Framework and Process

When considering the process for evaluating the risk management framework, agencies should ensure that it remains fit for purpose and consistent with the agency's objectives. Review methods will differ among agencies depending on:

- the maturity of the agency's risk management framework
- the resources available, and
- the aspect of the framework being assessed.

Review methods include a variety of self-assessment tools and internal audit processes. Further guidance on monitoring and review mechanisms can be found in the *Risk Management Toolkit for the NSW Public Sector* (TPP12-03) and the *Treasury Risk Maturity Assessment Tool*.

Risk Management Integration

1.2.5 Risk management integration is a fundamental principle of risk management and a key outcome of an effective risk management framework. It should be a dynamic and iterative process and customised to the agency's needs and culture. Risk management should be embedded within the agency's purpose, governance, leadership, commitments, strategy, objectives and operations. The Accountable Authority shall ensure, among other things, that:

- risk management is integrated into strategic and business planning, budgeting and reporting processes
- risks are formally considered when developing and implementing policies or programs, projects and other activities including procurement
- risk management is discussed as a regular agenda item at senior management meetings (minimum quarterly)
- risk management covers all relevant risk categories including strategic, operational, project, compliance, reputational, financial, legal and reporting risks
- the agency's ability to accept or tolerate risk is appropriately reflected in the internal control framework through, for example, financial and other delegations
- there is clear communication of risks and risk management practices to internal and external stakeholders
- there are agency-specific, fit-for-purpose tools, systems and processes to help all those responsible for managing risk.

Risk Management Culture

1.2.6 Risk management 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 agency. It is important that senior management take a leadership role in creating an environment that promotes positive risk management behaviour. The Accountable Authority shall ensure that:

- there is clear communication of risk management practices and their benefits
- senior managers demonstrate a commitment to risk management
- effective risk management is positively reinforced
- risk management capabilities are actively developed across the organisation
- measures of risk culture and attitude are incorporated into organisational climate surveys, risk maturity assessments[10] and performance management systems.

[10] Refer to the *Treasury Risk Maturity Assessment Tool Guidance Paper* (TPP20-06)

Practice Note – Positive risk management culture

Risk culture is the accepted set of shared values and behaviours that characterise how risk is managed within an agency. It drives how people recognise and respond to risks and opportunities. According to AS ISO 31000:2018, risk is managed in every part of the organisation's structure and everyone in an organisation has responsibility for managing risk. Risk management should be embedded in, and not separate from, the organisational culture, purpose, governance, leadership and commitment, strategy, objectives and operations. Therefore, in order to effectively implement a risk management framework and policy, agencies require a culture that emphasises at all levels the importance of managing risk as part of each employee's daily activities.

Many factors influence achieving a positive organisational culture, including the tone at the top, the code of conduct, and ethics and human resource policies. Examples of actions to support a positive risk culture include:

- The Accountable Authority and senior management setting and communicating the desired risk culture for the agency and regularly demonstrating their commitment to risk management by modelling expected risk management behaviours, providing adequate resources and continuously improving culture through key decision making, performance management and effective communication
- ARCs assessing and advising on the maturity of the agency's risk culture including monitoring the process for setting and measuring risk culture and seeking assurance that the agency, staff and relevant third parties are operating within the desired risk culture
- A defined approach to consider and manage risk across the agency which is commonly understood, agreed and used to drive risk-based decision making
- A culture of open communication is encouraged by senior management to ensure all employees feel comfortable and confident in speaking openly about risks, understand the agency's tolerance for risk and when and to whom risks should be escalated
- Designing agency-specific, fit-for-purpose risk management methodologies, tools, systems and processes to support effective risk management
- Ensuring risk registers are linked to agency objectives, are communicated in a timely and accurate manner to senior management and are integrated with business plans and/or performance agreements, to support decision making
- Regularly measuring, monitoring and reporting to senior management on risk culture, identifying desirable changes and taking steps to address these. This may be through organisational climate surveys, performance management systems and risk maturity assessments (refer to the below *Treasury Risk Maturity Assessment Tool*)
- Ensuring all employees (and contractors where appropriate) are provided with sufficient risk management training (role specific) and risk specialists have appropriate capabilities to design and implement the risk management framework
- Rewarding risk behaviours that effectively manage risk to agreed tolerances and managing poor behaviours
- Reviewing and monitoring risk management accountabilities and responsibilities as part of performance review processes
- Appointing a CRO who has a formal role in challenging risk decisions within the agency, is a member of the agency's senior management team and has access to the Accountable Authority and ARC.

Further tools and guidance

The *Treasury Risk Maturity Assessment Tool* (TPP20-06) supports the improvement of risk management, culture and capability across the NSW public sector. The tool provides agencies with a systematic, uniform approach for self-assessment that allows agencies to measure risk maturity, identify areas to improve, and communicate results to senior management and ARCs. Strategies based on the identified improvement areas may be developed to raise an agency's maturity to a targeted level and support improving their overall risk culture. Agencies are strongly encouraged to use the tool (at least annually) to identify areas of improvement and support uplifting their overall risk culture and capability.

The *Risk Management Toolkit for the NSW Public Sector* (TPP12-03) also provides further guidance on supporting a positive risk management culture.

Managing Project Risks

1.2.7 Sound project governance arrangements are key to managing project risks and should be proportionate to the level of risk taken.[11] The Accountable Authority shall ensure that the risk management process used to manage project risks is consistent with and linked to the agency's risk management framework, to ensure project risks are visible, rather than being managed as a discrete activity.

Risks that impact other agencies

1.2.8 The Accountable Authority shall implement processes to ensure that significant risks arising from the strategic and operational activities of the agency that affect, or are likely to affect, other agencies are formally communicated to the affected agencies.

1.2.9 In any communication relating to clause 1.2.8, the Accountable Authority shall include advice of any risk treatment measures that the agency has in place to manage the risk, and an assessment of any residual risk to the affected agencies. Further advice shall be provided if there are any material changes to this residual risk.

1.2.10 On receipt of advice from another agency about a risk that affects or is likely to affect an agency, the affected agency should make its own assessment of the risk and develop its own risk treatment strategy.

Emerging risks

1.2.11 When identifying risks as part of a risk assessment that might help or prevent an agency from achieving its objectives, agencies should continually assess their circumstances to identify new emerging types of risk and opportunities. Examples of contemporary emerging risks include climate related risks and cyber security risks.

1.2.12 Climate related risks should be considered when identifying types of risks that might impact an agency's ability to achieve its objectives. This type of risk should be considered as part of an agency's existing risk management framework and processes but may require additional considerations over and above a general risk assessment. Refer to the Department of Planning, Industry and Environment's Climate Risk Ready NSW Guide for further information on assessing climate related risks.[12]

1.2.13 Cyber security risks should be considered when identifying agency risks and embedded into the agency's risk management practices and assurance processes. Refer to the NSW Cyber Security Policy[13] for further information on establishing effective cyber security policies and procedures and ensuring cyber security risks to agency information and systems are managed.

---

11 For example, major projects should have more detailed risk analysis performed than small projects and be subject to assurance that is independent of the project delivery team/executive responsible for project delivery.

12 Department of Planning, Industry and Environment, Climate Risk Ready NSW Guide: Practical guidance for the NSW Government sector to assess and manage climate change risks (2020).

13 https://www.digital.nsw.gov.au/policy/cyber -security-policy#purpose--2791

2. Internal Audit Function

Principle 2:

An internal audit function should provide timely and useful information to management about:

- the adequacy of, and compliance with, the system of internal control
- whether agency results are consistent with established objectives, and
- whether operations or programs are being carried out as planned.

Core Requirements 2.1 – The Accountable Authority shall establish and maintain an internal audit function that is appropriate for the agency and fit for purpose.

Definition of Internal Audit

2.1.1 The 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 agency's operations. It helps an agency accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes".

2.1.2 The IIA definition covers two types of internal audit services:

- ***assurance services*** – an objective examination of evidence to provide an independent assessment of risk management, control and governance processes of the agency, and
- ***consulting services*** – advisory and related client activities, the nature and scope of which are agreed upon with the client and are intended to add value and improve an agency's governance, risk management and control processes without the internal auditor assuming management responsibility.

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

Establishment of Internal Audit Function

2.1.3 The Accountable Authority shall ensure there is an operational and adequately resourced internal audit function.

2.1.4 In the Policy, an 'internal audit function' means an 'in-house', a 'co-sourced' or an 'out-sourced' internal audit service delivery model. The Accountable Authority shall:

- determine the appropriate service delivery model for the internal audit function based on the agency's needs, which may change over time, and
- ensure that the service delivery model selected will provide assurance, independent from operational management, on risk management, control and governance processes.

Practice Note - Determining appropriate Service Delivery Models

When determining the most appropriate service delivery model for the internal audit function, agencies should consider the:

- size of agency, in terms of both staffing levels and budget
- complexity of the agency's core business
- risk profile of the agency's operations
- geographical and functional distribution of the agency's operations
- viability of alternative service delivery models and the ability of the agency to attract and retain suitable staff, including professional staff for in-house service delivery, and an experienced staff for out-sourced service delivery
- 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
- capacity of alternative service delivery models to deliver flexibility in the internal audit work-plan.

Practice Note - Service Delivery Models

Where the Accountable Authority 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 an agency's staff.

Where the Accountable Authority establishes the internal audit function using 'co-sourced' service delivery, the agency provides and manages internal audit services through a combination of in-house resources and contracted services delivered by an appropriately qualified third party provider.

Where an 'out-sourced' service delivery model is established, internal audit services are provided exclusively by an appropriately qualified third party provider.

A co-sourced or out-sourced service delivery model for the internal audit function may include utilisation by the Accountable Authority of pooled internal audit resources made available through, for example, a cluster arrangement.

2.1.5 Where the internal audit function is established using a co-sourced or out-sourced service delivery model, the Accountable Authority shall ensure that the agency's CAE is appointed as the liaison officer and/or contract manager for any internal audit services delivered by a third party provider. This is to ensure that the CAE retains control of the internal audit strategic direction and is able to actively monitor the performance of the third party provider.

2.1.6 In all models, responsibility for the internal audit function remains with the agency and the CAE, as described below, shall be an employee of the agency and cannot be outsourced, other than as a result of an appropriate shared arrangement.[14]

[14] In compliance with clause 2.1.13 or with the requirements of a Shared Arrangement as stated in this Policy. Refer to the Shared Arrangements section and Annexure G.

2.1.7 The Accountable Authority shall appoint a CAE to head the internal audit function. The CAE is the most senior officer within the agency with responsibility for internal audit.[15] The CAE position shall:

- be of a sufficient level of seniority to enable the CAE to fulfil their responsibilities in internal audit unimpeded, including being able to discuss and negotiate internal audit results with senior management on a reasonably equal footing[16]
- possess skills, knowledge[17] and personal qualities that can ensure the credibility and acceptance of the internal audit function
- not be out-sourced to a service provider.

2.1.8 In a Department,[18] the CAE shall have appropriate professional certifications[19] and qualifications and/or demonstrated relevant high-level experience for the oversight of a highly effective internal audit function and serve as a source of expert professional support to agencies across the cluster.

2.1.9 The Accountable Authority shall consult with the ARC when appointing, reappointing or removing a CAE.

2.1.10 The Accountable Authority shall determine whether the CAE position will be a dedicated role within the agency. In doing so, the Accountable Authority shall seek the advice of the ARC.

It is expected that a dedicated CAE position would be established where the agency has more than one of the following factors:

- significant assets
- a high risk profile
- a high level of expenditure
- engages in complex transactions.

2.1.11 Neither the Accountable Authority nor the CFO are to be appointed as the CAE.[20]

2.1.12 Where the appointed CAE also has responsibility for other aspects of the agency's operations that may possibly be the subject of an audit by the internal audit function, the agency shall implement safeguards to prevent an actual or perceived conflict of interest arising.

---

15 The only instance where a CAE might be appointed from outside the agency is in the case where a shared arrangement has been established under the provisions of this Policy.

16 It is not appropriate for the Accountable Authority or CFO to be appointed as the CAE as stated in 2.1.11.

17 It is recommended that the CAE should have appropriate professional certifications (may include those which would be recognised by the Institute of Internal Auditors, CPA Australia or Chartered Accountants Australia and New Zealand), qualifications and/or demonstrated relevant high-level experience for the oversight of an effective internal audit function.

18 For the purpose of this clause, 'Department' is limited to those entities listed in Schedule 1, Part 1 of the *Government Sector Employment Act 2013.*

19 Appropriate professional certification might include those which would be recognised by the Institute of Internal Auditors, CPA Australia or Chartered Accountants Australia and New Zealand.

20 Where an agency does not have a CFO, employees with a responsibility for the finances and/or financial reporting of the agency should not be appointed as CAE.

Practice Note - Safeguards to protect the independence and objectivity of Internal Audit

In situations where the CAE also has executive responsibility for other aspects of the agency's operations, such as compliance or risk management activities, agencies may consider implementing any or all of the following safeguards to preserve the independence and objectivity of internal audit:

- documenting any conflicts of interest (perceived or actual) concerning the other operational roles held by the CAE
- assigning the role usually performed by the CAE during an audit assignment of any operational area which is also the responsibility of the CAE, to another member of the executive who is independent of the internal audit function of the agency and retains the same level of seniority of the CAE
- where the audit assignment concerns any operational area which is also the responsibility of the CAE, ensuring that internal audit project briefs are reviewed by the ARC to ensure adequate coverage of the proposed audit
- where an agency engages service providers, providing mechanisms for the service providers to raise any identified or perceived conflicts of interest with the Accountable Authority, and then (if appropriate) the ARC, and
- periodic review of internal audit charters to reflect changes in roles and responsibilities.

2.1.13 A CAE may be shared, outside of the requirements and approval required for a Shared Arrangement as stated in this Policy, between more than one agency within a cluster where:

- there is a common accountable authority
- the CAE is a direct report to the accountable authority (administratively)
- the CAE is a dedicated role within one of the agencies, and
- the CAE heads the internal audit function for each agency and has sufficient internal resources available to him/her to properly deliver an in-house internal audit function or properly manage an outsourced or co-sourced internal audit function.

2.1.14 To achieve operational independence of the internal audit function, the Accountable Authority shall ensure that the CAE has a dual reporting line. A dual reporting line means that the CAE shall:

- report ***administratively*** to the Accountable Authority to facilitate day-to-day operations of the internal audit function,[21] and
- report ***functionally*** to the ARC for strategic direction and accountability of the internal audit function.

Where the Accountable Authority delegates the administrative reporting line, the Accountable Authority shall ensure the delegation is:

- to a Senior Executive who reports to the Accountable Authority,
- to a sufficient level of seniority to enable the CAE to fulfil their responsibilities in internal audit, and
- sufficiently independent of the CAE's role by demonstrating the implementation of the following safeguards:
    - the CAE shall have direct access to the Accountable Authority to discuss audit and risk issues and challenge decisions of the delegate as deemed required by the CAE
    - the ARC Chair contributes to the CAE's regular performance review

[21] In the case of a statutory body (included in the definition of GSF agency in the GSF Act section 2.4(1)(i), it may be appropriate for the CAE to report administratively to either the Accountable Authority of the statutory body or a delegate director of the board.

- the CAE shall not report administratively to the CFO
- When internal audit reports and the annual audit plan are submitted to the Accountable Authority, the CAE shall be able to:
  - consult with the ARC Chair on the internal audit findings and annual audit plan, and
  - submit to the Accountable Authority, without amendment by the administrative reporting line manager, the
    a) internal audit findings, recommendations and reports, and
    b) annual audit plan for approval.

The dual reporting line shall be consistent with the 'reporting line' structure in Figure 4 below. In Figure 4, the dotted line represents the 'administrative' reporting line and the bold line represents the 'functional' reporting line:

Figure 4: Dual reporting line structure

*Note: Under 1.1.6, internal audit is responsible for providing assurance to the Accountable Authority and the ARC on the effectiveness of the risk management framework. However, all agencies are encouraged to nominate a CRO who is responsible for the oversight and promotion of risk management within the agency, designing the agency's risk management framework and for the day-to-day activities of embedding the framework in the agency. The CRO or risk management function should report to either the Accountable Authority or a direct report to the Accountable Authority, such as a member of the executive with responsibility for governance or planning, so that independence of risk management from line management is maintained.

Where a CAE is shared, the CAE reports functionally to the ARC of each individual agency.

Practice Note – Reporting Lines

Administrative Reporting Line

Administratively reporting to the Accountable Authority may include:

- Approving the Internal Audit resources and annual budget (in consultation with the ARC)
- Provision of corporate services to Internal Audit including office accommodation, computers and equipment
- Human resource administration
- Administration of internal policies and procedures (e.g. expense approvals, leave approvals, floor space, etc.).

Functional Reporting Line

Functionally reporting to the ARC may include the Committee:

- Reviewing the Internal Audit Charter
- Recommending approval of the risk-based internal audit plan
- Receiving communications from the CAE on the internal audit activity's performance relative to its plan and other matters
- Reviewing reports on the results of internal audit engagements
- Providing advice to the Accountable Authority on the CAE's appointment or removal and their remuneration
- Making appropriate inquiries of the Accountable Authority and the CAE to determine whether there are inappropriate scope or resource limitations for internal audit.

Core Requirements 2.2 – The Accountable Authority shall ensure the internal audit function operates consistent with the International Standards for Professional Practice for Internal Auditing.

Consistency with International Standards for the Professional Practice of Internal Auditing

2.2.1 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 General Government Sector. The IIA Standards, and related professional practice guidelines, are available from the Institute of Internal Auditors website.[22]

2.2.2 The Accountable Authority shall ensure that the internal audit function, as defined in the 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 NSW Government policies and guidelines.

Additional Internal Audit Requirements

Internal Audit Policies and Procedures

2.2.3 The Accountable Authority shall ensure that the CAE develops and maintains policies and procedures for the internal audit function.[23]

[22] https://www.iia.org.au/technical-resources/professionalGuidance/standards.aspx

[23] An audit manual is considered equivalent for the purpose of satisfying the agency's requirement to maintain policies and procedures.

2.2.4 Where the internal audit function is established using a co-sourced or outsourced service delivery model, the Accountable Authority shall 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 policies and procedures
- apply audit methodologies that accord with the IIA Standards
- make the audit methodologies used accessible to the agency (subject to any licensing or other restrictions that may be in place).

The establishment of a co-sourced or outsourced service delivery model does not, however, discharge the requirement for the agency to develop and maintain policies and procedures for those structural elements, other than audit methodology, listed in clause 2.2.6 below.

2.2.5 The ARC shall review and provide advice to the Accountable Authority on the internal audit policies and procedures before those policies and procedures are finalised.

2.2.6 The internal audit policies and procedures shall be consistent with the Policy and the professional practices set out in the IIA Standards and include the following structural elements:

- general policies and standards including the Audit Charter
- structure, resourcing and professional development of the internal audit function
- audit planning including strategic and annual audit planning
- audit methodology
- audit reports
- recommendations and timeframes relating to monitoring and reporting
- internal audit quality assurance and improvement, and
- information management including document security.

2.2.7 All internal audit documentation is to remain the property of, and able to be accessed by, the audited agency including where the internal audit services are performed by an external third party provider.

Audit Reports

2.2.8 In addition to the requirements set out in the IIA Standards, the Accountable Authority shall ensure that the internal audit function, as defined in the Policy, operates in accordance with the requirements for the reporting and monitoring of internal audit activities set out in this Core Requirement.

2.2.9 The CAE shall report to the ARC those internal audit findings and related recommendations that are assessed to be the most significant using methodology that risk rates audit findings, as set out below (clauses 2.2.12 – 2.2.16).

2.2.10 The CAE shall ensure that the ARC has access to all internal audit findings, reports and related recommendations.

2.2.11 The CAE shall develop and maintain policies and procedures for the reporting of internal audit findings, recommendations and agreed action plans in the agency.

***Practice Note - Audit Reports**:*

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. It is noted that the IIA Standards require that communications be accurate, objective, clear, concise, constructive, complete and timely.

The policies and procedures for the reporting of internal audit findings and recommendations in the agency should be drafted to ensure that each Audit Report:

- contains an overall audit conclusion and risk rating related to the audit objective(s)
- contains risk-rated audit observations
- is prepared in accordance with a stipulated report template
- is drafted and finalised within stipulated timeframes
- includes comments from appropriate management
- includes an action plan, including the individual responsible and timeframe for implementing agreed recommendations, and
- contains details of the review and quality processes conducted.

Risk Rating of Audit Findings

2.2.12 The CAE shall ensure that the internal audit function adopts a methodology that risk rates audit findings for assessing and responding to audit issues. The methodology should be consistent with the current risk standard, as defined in Core Requirement 1.2 of the Policy.

2.2.13 The ARC shall review and endorse the methodology for risk rating audit findings. Once finalised, the methodology shall be the basis for protocols relating to the reporting of audit findings, monitoring of the implementation of agreed actions and the follow-up of outstanding agreed actions.

2.2.14 The CAE shall ensure that every audit finding is categorised and prioritised according to the risk the audit finding represents to the agency if the recommendations related to the finding are not implemented.

2.2.15 The CAE shall ensure that a common, easily understood system for risk categorisation is used to communicate the relative importance of the risk ratings of findings to the ARC, the Accountable Authority and operational management.

Practice Note - Risk categorisations for audit findings

It is good practice for agencies to align their risk categorisation system for audit findings with the categorisation system used in the agency's risk management framework. This can help with the agency's understanding of risk. Where this is not feasible or appropriate, agencies should ensure that the relationship and differences between various categorisation systems are clearly identified.

2.2.16 The ARC shall review the audit findings and related recommendations that have been assessed as the most significant according to the risk.

Action Plans

2.2.17 The CAE shall ensure that a course of action is recommended for every audit finding.

2.2.18 The CAE shall ensure identified issues and recommended actions are discussed with and referred to operational management for a formal response. Operational management will

determine appropriate action and should consult with the CAE where relevant, but has a right to elect to take no action. Management's proposed action and any reasons for taking no action shall be documented in the audit report.

2.2.19 The Accountable Authority shall ensure that operational management prepares an action plan for every internal audit. The action plan shall assign responsibility for implementation to individuals within the agency.

2.2.20 The Accountable Authority shall ensure that all actions are implemented within proposed timeframes.

Monitoring and follow-up of Action Plans

2.2.21 The CAE shall establish and maintain a system to monitor and follow-up progress in implementing action plans. The system should be documented in policies and procedures required under clauses 2.2.3 – 2.2.7 above.

2.2.22 The CAE shall report on the progress of the implementation of the action plans to the ARC.

2.2.23 Where the ARC is not satisfied with progress in implementing actions, the ARC shall refer the concerns to operational management and, where necessary, the Accountable Authority so that operational management is made fully aware of the risks posed to the agency.

Core Requirements 2.3 – The Accountable Authority shall ensure the agency has an Internal Audit Charter that is consistent with the content of the 'model charter'.

Model Charter for the Internal Audit Function

2.3.1 The Accountable Authority shall ensure that the internal audit function has a Charter that contains the structural elements of, and is consistent with, the content of the 'model charter' at Annexure A of the Policy.

2.3.2 The Internal Audit Charter shall be developed by the CAE and approved by the Accountable Authority on the recommendation of the ARC.

2.3.3 The Accountable Authority is required to consider the specific circumstances of the agency and may, where appropriate, include provisions additional to those set out in the model charter providing these do not conflict with the model charter.

Governance of the Internal Audit Function

2.3.4 The Accountable Authority shall ensure there is a clear separation of operational management from the internal audit function.

2.3.5 As noted in 2.1.14 above, to achieve operational independence of the internal audit function, the Accountable Authority shall ensure that the CAE has a dual reporting line.

2.3.6 The Accountable Authority shall ensure that internal audit reporting lines are clearly documented within the Internal Audit Charter and ARC Charter.

2.3.7 The ARC shall review and make recommendations regarding the approval of internal audit plans to the Accountable Authority.

2.3.8 The Accountable Authority shall ensure that the internal audit function is appropriately positioned within the agency's governance framework to work with external audit and internal business units.

2.3.9 The Accountable Authority shall ensure that the internal audit function is operationally independent from the activities it audits.

Resourcing of the Internal Audit Function

2.3.10 The Accountable Authority shall ensure that the internal audit function has a budget and access to sufficient professional resources with the necessary capabilities, skills and experience that are sufficient relative to the risks and assurance needs of the agency.

2.3.11 The Accountable Authority shall determine the budget and level of resourcing taking into account recommendations made by the ARC.

Where the ARC considers that the level of resourcing for the internal audit function is insufficient relative to the risks facing the agency, it should draw this to the attention of the Accountable Authority. The chair of the ARC shall ensure that the Committee's review of, and recommendations on, proposed allocations of resources are minuted by the Committee's secretariat.

2.3.12 The Accountable Authority shall 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), CPA Australia (CPA) and Chartered Accountants Australia and New Zealand (CA).

2.3.13 The Accountable Authority shall ensure that all internal audit staff are provided with sufficient and up-to-date information on the agency's objectives, risks and operations in order for them to perform their roles and discharge their responsibilities.

Practice Note - Training and development for staff of the internal audit function

The CAE should, as part of strategic planning for the internal audit function, identify the training and development needs of professional and other staff of the internal audit function including:

- the professional development needs of professional staff
- the training and development needs of other staff in order to effectively discharge their roles and responsibilities including, where a co-sourced or outsourced service delivery model is adopted, ensuring staff are equipped as informed clients in liaising with external service providers
- learning and development activities to enhance the capabilities of staff, together with their understanding and awareness of governance, risk and control issues affecting the agency.

The CAE should ensure that these training needs are undertaken.

Internal Audit Quality Assurance and Improvement

2.3.14 The Accountable Authority shall ensure there is a documented and operational Quality Assurance and Improvement Program for the internal audit function.[24]

2.3.15 The agency's Quality Assurance and Improvement Program shall include both internal and external assessments. Internal assessments shall include:

- ongoing monitoring of the performance of the internal audit function, and

[24] This requirement applies regardless of the Internal Audit service delivery model adopted.

- at least annual self-assessments or assessment by other persons within the agency with sufficient knowledge of internal audit practices.

2.3.16 An external assessment of the internal audit function shall be conducted at least once every five (5) years by a qualified, independent assessor selected in consultation with the ARC. That review shall consider the agency's compliance with and performance against the Policy and the relevant professional standards.

Practice Note - Nature of external assessment of internal audit function

The internal audit function of the agency should operate in accordance with the professional standards and focus on delivering outcomes for the agency. This assessment should be carried out even where the majority of the internal audit function is outsourced to an external service provider. The assessment is not of the external service provider but rather on the internal audit function as implemented in the agency.

It is envisaged that an agency would commission an external assessment that would cover both those areas that are delivered internally (e.g. whether the Agency has an Internal Audit Charter and whether the results of audits are communicated and disseminated to appropriate parties within the agency) and those that are delivered by an external service provider (e.g. whether engagements have been performed with proficiency and due professional care). A significant component of the assessment would be whether the internal audit activity has evaluated and contributed to the improvement of governance, risk management and control processes within the agency.

The external service provider might have its own quality accreditation that an agency may require evidence of as part of the engagement process. This will, however, be unrelated to assessment of the internal audit function required by clauses 2.3.14 - 2.3.16.

Practice Note - Process of external assessment of internal audit function

An external assessment can be undertaken by:

1. engaging an external assessor to undertake the assessment
2. undertaking a self-assessment and engaging a qualified external reviewer to conduct an independent validation of that self-assessment.

It is recognised that some agencies may incur a significant cost burden associated with an independent external engagement for the purposes of conducting an external review of the internal audit function. In these circumstances, appropriate alternative arrangements may include establishing an arrangement with another agency or agencies to provide external review services.[25] When entering these arrangements, the Accountable Authority shall consider both the independence[26] and expertise of the assessor or assessment team.

2.3.17 The results of the external assessment shall be reported to the ARC for advice to the Accountable Authority on the results.

[25] Please note that such arrangements are not permitted to be reciprocal in nature as this would not satisfy independence requirements with respect to external assessment. Agencies wishing to collaborate for the purposes of conducting an external assessment may wish to consider arrangements involving three or more agencies.

[26] This Policy adopts the definition of independence provided by the IIA *International Professional Practices Framework, Implementation Guide 1312 - External Assessments* for the purposes of external assessment of the internal audit function as "not having either an actual or a perceived conflict of interest and not being part of, or under the control of, the organisation to which the internal audit activity belongs".

3. Audit and Risk Committee

Principle 3:

An independent Audit and Risk Committee with appropriate expertise should provide relevant and timely advice to the Accountable Authority on the agency's governance, risk and control frameworks and its external accountability obligations.

Core Requirements 3.1 – The Accountable Authority shall establish and maintain efficient and effective arrangements for independent Audit and Risk Committee oversight to provide advice and guidance to the Accountable Authority on the agency's governance processes, risk management and control frameworks, and its external accountability obligations.

Establishment of an Audit and Risk Committee

3.1.1 The Accountable Authority shall establish efficient and effective arrangements for an ARC to oversee and monitor governance, risk and control issues affecting the operations of the agency.

3.1.2 When considering the most efficient and effective arrangements for ARC oversight, a shared ARC can be a means of providing ARC oversight for a number of agencies. The Cluster Secretary should ensure efficient and effective oversight arrangements are established within their cluster and sufficient advice and guidance is provided to each agency's Accountable Authority on the agency's governance processes, risk management and control frameworks, and its external accountability obligations.

3.1.3 The Cluster Secretary should consult with each Accountable Authority (except agencies defined as Special Offices) in their cluster to:

a) first consider whether an agency may enter into a Principal Department Led Shared ARC; or

b) if specific circumstances are met, consider forming a Collaborative Shared ARC or standalone ARC.

Specific circumstances where it may be more appropriate to form a collaborative shared ARC or a standalone ARC (rather than a Principal Department led ARC) include:

- All Requirements of a Principal Department Led ARC cannot be met
- Agency is a Special Office
- Agency has a role that requires independence from other agencies
- Agency's risk profile warrants standalone arrangements
- Secrecy provisions applicable to an agency could be breached if they enter a shared arrangement.

3.1.4 If an Accountable Authority decides to enter their agency into a Shared Arrangement, including a shared ARC, the requirements of a Shared Arrangement which are detailed in Annexure G: Shared Arrangements shall be followed including the:

- Requirements of a Principal Led or Collaborative Shared ARC are met (refer to the Shared Arrangements - section A. Shared ARCs), and/or
- Requirements of sharing a CAE and/or Internal Audit function are met, if applicable (refer to the Shared Arrangements - B. Shared CAE or Internal Audit function), and
- Shared Arrangements Agreement is signed by all Accountable Authorities in the Shared Arrangement, and
- Cluster Secretary approves the Shared Arrangement.

3.1.5 The ARC shall have no fewer than three (3) members and no more than five (5) members.[27] Depending on the size and complexity of the agency, and if applicable, the size and complexity of a shared ARC, more than three members may be required for the committee to effectively discharge its responsibilities.[28]

3.1.6 The Accountable Authority shall appoint the chair[29] and members of the ARC from the panel of pre-qualified individuals.[30]

Practice Note - Appointment of members from the Prequalification Scheme

Department of Premier and Cabinet Circular No. C2009-13 established the *Prequalification Scheme: Audit and Risk Committee Independent Chairs and Members.* Instructions in the Policy should be read in conjunction with the Scheme Guidelines and any accompanying conditions and guidelines, as updated from time to time. Scheme documentation can be found on the buy.nsw website.

Independence of members

3.1.7 The Accountable Authority shall appoint only 'independent members' (including an 'independent chair') to the agency's ARC from the panel of pre-qualified individuals. 'Independence' requirements are listed in clause 3.1.8.[31]

3.1.8 Members of the ARC will be classified as being 'independent members' except if they possess any of the following relationships:[32]

- is currently employed in the NSW government sector,[33] except as a non-executive director of a governing board of a statutory body[34]
- has been employed in a senior management role[35] in the appointing agency or associated agency within the last three years
- has been employed in the NSW government sector in a role that can exert direct and significant influence over a service provider to the appointing agency within the last three years

27 Inclusive of the Chair.

28 The maximum remains five (5) Audit and Risk Committee members, inclusive of the Chair.

29 An individual shall be pre-qualified as a chair on the Prequalification Scheme: Audit and Risk Committee Independent Chairs and Members to be appointed as a chair. An individual who is pre-qualified as a member only cannot be appointed as a chair to an Audit and Risk Committee.

30 The Prequalification Scheme: Audit and Risk Committee Independent Chairs and Members. Refer to the Prequalification Scheme: Audit and Risk Committee Independent Chairs and Members – Conditions – December 2020 and Guidelines – December 2020.

31 Prequalification does not preclude the need for the Chair and members to satisfy the requirement to be independent.

32 The 'conflict of interest' relationships listed in clause 3.1.8 draw on the independence guidelines set out in Accounting Professional and Ethical Standards Board, APES110: *Code of Ethics for Professional Accountants (including Independence Standards)*, November 2018.

33 Government sector as defined in the *Government Sector Employment Act 2013.*

34 Current employees of all NSW government sector agencies cannot serve as members or chairs of an Audit and Risk Committee, including within their own agency. This includes statutory and special appointments other than non-executive directors of the governing board of a statutory body (which is included in the definition of GSF agency in the GSF Act section 2.4(1)(i)). This excludes being an "employee" within the extended meaning in the *Superannuation Guarantee (Administration) Act 1992 (Cth)* as a result of being engaged as an ARC member or chair under the Prequalification Scheme for the purposes of this Policy.

35 Excluding as non-executive directors of the governing board of a statutory body (included in the definition of GSF agency in the GSF Act section 2.4(1)(i)).

- currently performs, or has performed, any services including advisory roles, for an agency which directly affects the subject matter of the ARC of the appointing agency within the last three years[36]
- has a material business or other contractual relationship or any other direct financial interest or material indirect financial interest with the appointing agency or an associated agency, which could reasonably be perceived to materially interfere with the individual's ability to act in the best interests of the appointing agency
- currently acts, or has acted as an advocate of a material interest on behalf of the appointing agency, or an associated agency, or currently is or has been engaged in litigation or in resolving disputes between the appointing agency and third parties
- has an immediate family member or close family member[37] who is employed in a senior management role of the appointing agency or an associated agency, or is employed in any other role which can exert direct and significant influence over the subject matter of the ARC of the appointing agency.

This list prescribes the minimum key relationships that shall be avoided. The appointing Accountable Authority shall ensure appropriate safeguards are in place to eliminate or reduce significant threats to independence in accordance with the terms of this clause.

Practice Note – Independence of ARC Members in Principal Department Led Shared ARCs

When ensuring appropriate safeguards are in place to protect the independence of ARC members and chairs, the Accountable Authority should specifically consider safeguards for ARC members and chairs that are appointed to a **Principal Department Led Shared ARC**.

There are several factors which may impact the independence of a member or chair including:

- The size and complexity of this type of committee as it oversees a Department and multiple agencies in a cluster. The members and chair will have oversight over a significant proportion of a cluster which may increase the familiarity threat to independence
- If a member or chair were to be appointed to an ARC in another cluster, this increases their commitment and stake in NSW Government which could increase the self-interest and familiarity threat to independence and may be comparable to the independence requirement against members being NSW Government employees.

Appropriate safeguards for Principal Department Led Shared ARCs may include:

- ARC members and chairs being appointed to no more than one Principal Department Led Shared ARC
- Considering to not extend these ARC members and chairs beyond five (5) years
- Occasionally undertaking an external performance review of the ARC if the majority of performance reviews are self-assessments.

These safeguards will also support ensuring that members and chairs have sufficient capacity to cover the entities they oversight.

Refer to Annexure G for further information on Principal Department Led Shared ARCs.

[36] This does not include non-executive directors of a governing board of a statutory body; such non-executive directors are considered independent members under this Policy if the remaining independence requirements in 3.1.8 are met.

[37] Immediate family member or close family member are defined in Accounting Professional and Ethical Standards Board, APES110: *Code of Ethics for Professional Accountants (including Independence Standards)*, November 2018.

3.1.9 For the purposes of clause 3.1.8, non-executive directors of the governing board of a statutory body that are pre-qualified in accordance with clause 3.1.6 are not considered to be 'employed' by an agency and are eligible for appointment as chairs and members of the ARC provided that they meet the other independence requirements provided in clause 3.1.8.

3.1.10 The Accountable Authority shall ensure that adequate procedures are in place to preserve the independence of the chair and members of the ARC.

3.1.11 The chair and members of the ARC shall notify the Accountable Authority immediately if an actual or perceived threat to their independence arises.

Qualification of members

3.1.12 When selecting ARC members, the Accountable Authority shall consider their suitability to the specific needs of the agency but also take reasonable steps to ensure that members collectively possess and maintain, the following skills and knowledge:

- extensive knowledge of the governance and financial management of agencies in the General Government Sector
- exceptional financial literacy, including the ability to understand and appropriately interrogate financial statements
- an understanding of the objectives and responsibilities of agencies
- a functional, contemporary and operational knowledge of:
    - risk management
    - performance management frameworks
    - internal audit
    - external audit
    - financial management
    - accounting
    - internal control frameworks
    - governance (including planning, reporting and oversight), and
    - legal and compliance frameworks.
- up to date training and professional development through relevant professional associations, e.g. Institute of Internal Auditors (IIA), CPA Australia (CPA), Chartered Accountants Australia and New Zealand (CA) and Australian Institute of Company Directors (AICD).
- capacity to ensure the integrity of the decision making of the ARC, including a willingness to constructively challenge management practices and information
- unwavering professionalism and ethical behaviour which exemplifies the culture of the NSW Public Service within the framework of Government Sector Core Values in section 7 of the *Government Sector Employment Act 2013*.

Terms of Members

3.1.13 The initial term of membership of the ARC shall be at least three (3) years and shall not exceed five (5) years.

3.1.14 Members can be reappointed or extended for further term(s) but the total period of continuous membership on the Committee shall not exceed eight (8) years (inclusive of any term as chair of the Committee).[38]

[38] Refer to clause 3.1.16.

3.1.15 Any reappointment or extension of membership on the ARC shall be approved only after the Accountable Authority has made a formal assessment of the member's performance as a committee member.

Practice Note - Staggering member renewal dates

Continuity of knowledge and experience on the Audit and Risk Committee is integral to its effective operation. It is strongly recommended that membership renewal dates 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.

Terms of Chairs

3.1.16 The chair of the ARC shall be appointed for one (1) term only for a period of at least three (3) years, with a maximum period of five (5) years. The term of appointment for the chair can be extended but any extension shall not cause the total term to exceed five (5) years as a chair of the ARC.

Practice Note - The term of the chair

A member of the *Prequalification Scheme: Audit and Risk Committee Independent Chairs and Members*, who has been prequalified as a chair, may be appointed as a chair either prior to or subsequent to a term as a member. However, the member's total term as chair shall not exceed five (5) years and the member's total term on the Committee (inclusive of a term as chair and a term as a member) shall not exceed a total of eight (8) years.

For example, a member of the Prequalification Scheme might be appointed for an initial term of three (3) years as a member and then be appointed as chair of the Committee for a period of five (5) years or vice versa.

Supplementary Terms

3.1.17 Individuals who have served a term of eight (8) years (including a term as chair (as relevant)) on the ARC of an agency may be reappointed for a further eight (8) year term with the same agency provided that the individual has served a period of three (3) years during which they have not been appointed to the agency's ARC. Their reappointment is also subject to the individual also meeting the independence requirements of the Policy in clause 3.1.8 and remaining pre-qualified in accordance with clause 3.1.6.[39]

Purpose of Audit and Risk Committee

3.1.18 The objective of the ARC is to provide independent assistance to the Accountable Authority by monitoring, reviewing and providing advice and guidance about the agency's governance processes, risk management and control frameworks and its external accountability obligations.

Responsibilities of Audit and Risk Committee

3.1.19 The ARC is an integral component of an agency's corporate governance arrangements and its responsibilities will generally cover the review and overview of the following areas:

- internal controls

[39] This clause applies only to individuals seeking to be reappointed to the Audit and Risk Committee of an agency to which they have previously been appointed and they have already completed a term of eight (8) years (including any term as chair of the agency's Audit and Risk Committee).

- risk management
- corruption and fraud prevention
- external accountability (including the financial statements)
- applicable laws and regulations
- internal audit[40]
- external audit.

3.1.20 The ARC is also expected to overview the agency's financial information, which includes mandated reviews of the agency's:

- processes for management review and consideration of the financial position and performance of the agency including the frequency and nature of that review (including the approach taken to addressing variances and budget risks)
- CFO Letter of Certification and supporting documentation (consistent with Treasury Policy *Certifying the Effectiveness of Internal Controls Over Financial Information* (TPP17-06))
- early close procedures and pro-forma financial statements
- cash management processes
- processes for collection, management and disbursement of grants and tied funding.

3.1.21 The ARC has no executive powers.

3.1.22 The ARC does not have delegated financial responsibility or any management functions.

Subcommittees of an Audit and Risk Committee

3.1.23 A Subcommittee may be established to support an existing ARC. The establishment of a Subcommittee is optional. A Subcommittee can be standing (ongoing) or time limited.

3.1.24 A Subcommittee may be established to oversee functions, divisions or business areas of an agency, or to oversee specific projects. Reporting into the ARC, a Subcommittee may consider the detail and provide summaries and proposals for the ARC to consider. This can assist the ARC to perform its responsibilities effectively and not be overwhelmed by the volume of issues.

3.1.25 An ARC cannot delegate its responsibilities to a Subcommittee. While the ARC may delegate tasks and functions to Subcommittees, the ARC retains full responsibility for oversight of the entity(ies). A Subcommittee should not be established as a surrogate ARC to oversee one or more legal entities within a cluster.

3.1.26 A Subcommittee can only be established with the approval of the Accountable Authority. Following consultation with the ARC, an Accountable Authority may also decide that a Subcommittee is no longer required.

3.1.27 The Chair of the Subcommittee should be an independent pre-qualified member of the ARC (but does not need to be pre-qualified as a Chair under the Prequalification Scheme). It is strongly recommended that:

[40] As referred to in 2.3.11, where the ARC considers that the level of resourcing for the internal audit function is insufficient relative to the risks facing the agency, it should draw this to the attention of the Accountable Authority. The ARC Chair shall ensure that the Committee's review of, and recommendations on, proposed allocations of resources are minuted by the Committee's secretariat.

- the Chair of the ARC not be the Chair of the Subcommittee to avoid the situation of the Chair reporting to him/herself, and
- the Subcommittee is comprised of a majority of independent members.

3.1.28 Independent members of the Subcommittee may be selected from the ARC or the Prequalification Panel. In exceptional circumstances, where specialist skills are required and are not available from the Prequalification Panel, independent members on the Subcommittee may be selected from outside the Prequalification Scheme.

3.1.29 The Accountable Authority, the CAE and the CFO shall not be members of the Subcommittee but may attend meetings as observers as determined by the Chair.

3.1.30 The remuneration of the Chair and members of a subcommittee shall be in accordance with the Prequalification Scheme conditions. Total expenditure of the function/business area/division or specific project overseen by the Subcommittee should be established. The maximum remuneration of the Chair and members of a Subcommittee shall be determined based on the remuneration applicable to an agency of equivalent size in accordance with the Prequalification Scheme conditions. The annual fee structure applicable to the Chair should be prorated based on the life of the committee where the Subcommittee is not ongoing.

3.1.31 Membership of a Subcommittee by an independent member of the ARC of that agency will not count for the purposes of the Prequalification Scheme condition clause 11.5 that limits pre-qualified independent members to membership of no more than five (5) ARCs.

Core Requirements 3.2 – The Accountable Authority shall ensure the Audit and Risk Committee has a Charter that is consistent with the content of the 'model charter'.

Model Charter for Audit and Risk Committee

3.2.1 The Accountable Authority shall ensure that the ARC has a Charter that is consistent with the content of the model charter at Annexure B of the Policy.

3.2.2 The Accountable Authority is required to consider the specific circumstances of the agency and may, where appropriate, include provisions additional to those set out in the model charter providing these do not conflict with the model charter.

3.2.3 The Accountable Authority shall approve the Charter and ensure it has been distributed to all members of the ARC, including all new appointments.

3.2.4 The ARC shall ensure that:

- the Charter is formally reviewed by the ARC periodically, at least annually, to ensure its ongoing relevance, recommend updates for approval by the Accountable Authority
- the Charter is sufficiently detailed to ensure there is no ambiguity
- the Charter has clear guidance on key aspects of the committee's operations.

Audit and Risk Committee Operations

3.2.5 The ARC shall meet at least quarterly. Depending on the size and complexity of the agency and if applicable, the number and complexity of agencies in a shared ARC, more frequent meetings may be necessary in order for the ARC to effectively perform its roles and discharge its responsibilities.

3.2.6 The Accountable Authority shall nominate a person(s) to provide secretariat support to the ARC.

3.2.7 The appointed secretariat support is responsible for minuting the meetings of the ARC. The minutes shall include a record of attendance, issues, outcomes (including decisions) and action items.

3.2.8 Accountable Authorities are encouraged to attend the meetings of the ARC. Committee members, if necessary, are able to have in-camera discussions.[41] The chair of the ARC should indicate prior to the meeting which agenda items may be of particular interest to the Accountable Authority.[42]

3.2.9 Nothing in the Policy prevents the CAE, CRO (as relevant), external audit representatives and any other agency representatives from attending ARC meetings, except where the Committee members wish to have in-camera discussions.

3.2.10 The minutes of meetings of the ARC shall be provided to the Accountable Authority within a reasonable time frame, as agreed between the ARC and the Accountable Authority. The agreed time frame shall be stated in the ARC's Charter.

Practice Note - Providing minutes to the Accountable Authority

It is good practice to provide the minutes of the ARC meeting within two (2) weeks of the meeting date to the Accountable Authority.

3.2.11 The Accountable Authority is responsible for ensuring that the ARC is promptly provided with all necessary and relevant information regarding their responsibilities and operations both prior to and during their appointment to enable them to develop and maintain a sound understanding of the:

- business of the agency
- environment in which the agency operates, and
- contribution that the ARC makes to the agency.

Practice Note - Keeping the ARC up-to-date

Agencies are encouraged to implement processes and systems which enable their ARCs to remain up-to-date with developments concerning the General Government Sector relating to the ARC's responsibilities, together with significant compliance, strategic and operations matters affecting the agency.

For example, an agency may wish to consider including ARC members on their distribution lists for key circulars and policies issued by all central agencies, or providing briefings or access to briefings for Committee members on matters relevant to audit and risk.

3.2.12 The ARC is to have access to operational and senior management, including the CFO and/or Senior Accounting Officers when required. The Committee may request the CFO or other employees to attend Committee meetings or participate for certain agenda items.

3.2.13 The ARC may identify the need for independent expert advice and may request for the Accountable Authority to make such expert assistance available.

---

41 In the case of a governing board, the chair or a member may attend on behalf of the board, or the board may ask a nominated delegate to attend on its behalf.

42 The Accountable Authority is not considered a member of the ARC.

3.2.14 The ARC shall have direct access (where necessary) to the internal and external auditors without operational management being present and shall meet with the internal and external auditors at least annually.

Practice Note - Internal and external auditors

It is good practice for agencies to ensure that processes are in place to enable both the internal audit and external auditors to provide feedback to the ARC without management or other parties being present.

3.2.15 The ARC can seek explanations and additional information from any employee or contractor of the agency.

Reporting

3.2.16 The Accountable Authority shall ensure that processes are in place to allow the Committee, at any time, to report on any matters it deems of sufficient importance. In addition, processes should be established to allow an individual Committee member to request a meeting with the Accountable Authority.

3.2.17 The Committee shall at all times ensure it maintains a direct reporting line to and from internal audit and acts as a mechanism for internal audit to report to the Accountable Authority on functional matters.

3.2.18 The Committee will report at least once a year, to the Accountable Authority on its operation and activities during the year.

Practice Note - Annual report to the Accountable Authority

The report should include:

- an overall assessment of the agency's risk, control and compliance framework, including details of any significant emerging risks or legislative changes impacting the agency
- a summary of the work the Committee performed to discharge its responsibilities during the preceding year
- details of meetings, including the number of meetings held during the relevant period, the number of meetings each member attended and any conflicts of interest declared
- a summary of the agency's progress in addressing the findings and recommendations made in internal and external reports including any risk treatment strategies applied
- a summary of the Committee's assessment of the performance of internal audit
- results of the Performance Review of the Audit and Risk Committee as detailed in 3.2.21
- note the expiry of any ARC member or chair terms during the next financial year.

Conduct of Audit and Risk Committee Members

3.2.19 Members of ARCs shall act in accordance with the relevant codes of conduct that apply to public sector employees.

Practice Note - Conduct of ARC Members

Members of the ARC are subject to the general principles of conduct that apply to public sector employees. Members shall familiarise themselves with the relevant policies and guidelines, including:

- Code of Conduct: Audit and Risk Committee Chairs and Members
- Government Sector Core Values in section 7 of the *Government Sector Employment Act 2013*, and
- relevant agency codes of conduct.

Dispute Resolution

3.2.20 Where a dispute arises relating to a recommendation made to the Accountable Authority by the ARC in the execution of its role and responsibilities cannot be resolved, the chair of the ARC may make an oral or written request to the Secretary, Treasury for assistance to facilitate resolution of the matter. Where Secretary, Treasury may have a conflict of interest, the matter should be referred to the Secretary, Department of Premier and Cabinet.

Practice Note - Dispute resolution

It is important that the chair and members of the ARC develop, establish and maintain an effective working relationship with the agency's operational management, including the Accountable Authority. The chair and members of the ARC shall seek to resolve differences or concerns with operational management, including the Accountable Authority, by way of open negotiation.

Performance Review of the Audit and Risk Committee

3.2.21 The Accountable Authority, in consultation with the chair of the ARC, shall establish a mechanism to review and report on the performance of the ARC as a whole and the performance of the chair and each member at least annually.

Practice Note - Performance review of the ARC

The purpose of the review mechanism is to establish a robust quality assurance and improvement process that ensures the ARC continues to deliver on its Charter.

In a majority of instances, the performance review will be undertaken on a self-assessment basis, unless the Accountable Authority determines that an external review is warranted.

3.2.22 The review should assess the performance of the ARC and the performance of the chair and members against the Committee's Charter, and may include appropriate input from the Accountable Authority, operational management, the internal and external auditors and any other stakeholders.

3.2.23 In respect of the performance of the ARC as a whole, the results of the review shall be provided to the Accountable Authority to consider the findings and any recommendations of the review and, if required, ensure appropriate action is taken to improve the ARC's performance.

3.2.24 The Accountable Authority may delegate the performance review function set out in clause 3.2.21 (excluding review of the chair's performance) to the ARC chair, although ultimate responsibility for the integrity of the review mechanism, including the actioning of findings, rests with the Accountable Authority.

3.2.25 In respect of the performance of members of the ARC (excluding the chair), the results of the review shall be provided to the Accountable Authority, and the chair of the ARC shall provide formal feedback to Committee members on their performance.

3.2.26 In respect of the performance of the chair of the ARC, the results of the chair's self-assessment shall be provided to the Accountable Authority who shall then provide formal feedback to the chair on his or her performance.

Annexure A

Model Internal Audit Charter[43]

The Internal Audit functions of NSW agencies are 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 Accountable Authority and the Audit and Risk Committee, their existing Internal Audit Charter against this model. In doing so it is important that each agency 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 agency, and reflects developments in Internal Audit professional practices.

Introduction

The [Accountable Authority] has established the [name of internal audit unit] as a key component of the [agency]'s governance framework.

This charter provides the framework for the conduct of the internal audit function in the [agency] and has been approved by the [Accountable Authority] taking into account 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 agency's operations. It helps an agency accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.[44]

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

- provide assurance to the [Accountable Authority], and the Audit and Risk Committee, that the [agency]'s financial and operational controls, designed to manage the agency's risks and achieve the entity's objectives, are operating in an efficient, effective and ethical manner, and
- assist management in improving the agency's business performance.

Independence

Independence is essential to the effectiveness of the internal audit function. Internal audit activity shall be independent, and internal auditors shall be objective in performing their work. Internal auditors shall 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

[43] 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*. Copyright Commonwealth of Australia reproduced by permission.

[44] As defined by the International Standards for the Professional Practice of Internal Auditing (IIA) (2017). Where relevant, sections of this Charter also incorporate other elements of the International Standards for the Professional Practice of Internal Auditing.

does not prepare records or engage in original line processing functions or activities [except in carrying out its own functions].

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 [Accountable Authority][45] to facilitate day to day operations. The Chief Audit Executive has direct access to the Accountable Authority to discuss audit and risk issues when required.

The following dual reporting line is prescribed where the dotted line represents the 'administrative' reporting line and the bold line represents the 'functional' reporting line:

*Note: Internal audit is responsible for providing assurance to the Accountable Authority and the Audit and Risk Committee on the effectiveness of the risk management framework. However, all agencies are encouraged to nominate a CRO who is responsible for the oversight and promotion of risk management within the agency, designing the agency's risk management framework and for the day-to-day activities of embedding the framework in the agency. The CRO or risk management function should report to either the Accountable Authority or a direct report to the Accountable Authority, such as a member of the executive with responsibility for governance or planning, so that independence of risk management from line management is maintained.

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.[46] When responding to requests, agency staff and contractors should cooperate with the internal audit function and must not knowingly mislead the internal audit function or wilfully obstruct any audit activity.

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 [agency], including where internal audit services are performed by an external third party provider.

[45] Where a Shared Arrangement has been established in compliance with the *Internal Audit and Risk Management Policy for the General Government Sector*, the appropriate Accountable Authority should be identified.

[46] Subject to any overriding legislative restrictions on information.

Roles and responsibilities

The internal audit function shall 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, and contribute to the improvement, of risk management processes
- provide assurance to the Accountable Authority and the ARC on the effectiveness of the risk management framework including the design and operational effectiveness of internal controls
- provide assurance that risk exposures relating to the agency'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 agency's ethics-related objectives, programs and activities
- assess whether the information technology governance of the agency sustains and supports the agency's strategies and objectives.

Compliance

- compliance with applicable laws, regulations and Government policies and directions.

Performance improvement

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

Advisory services

The internal audit function can advise the [agency]'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 treatment and monitoring strategies as part of the risk management framework

Fraud and corruption control

- evaluate the potential for the occurrence of fraud and how the agency manages fraud risk
- assisting management to investigate fraud, identify the risks of fraud and develop fraud prevention and monitoring strategies
- develop, implement and maintain a fraud and corruption control framework to prevent, detect and manage fraud and corruption.

Audit support activities

The internal audit function is also responsible for:

- managing the internal audit function
- assisting the Audit and Risk Committee to discharge its responsibilities
- 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 may cover all programs and activities of the [agency] 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 this Charter, the Internal Audit and Risk Management Policy for the General Government Sector and with relevant professional standards including International Standards for the Professional Practice of Internal Auditing issued by the Institute of Internal Auditors.

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. This includes consideration of current activities, trends and emerging issues, to enable relevant advice and recommendations
- 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 a risk-based annual internal audit work plan in a form and in accordance with a timetable agreed with the Audit and Risk 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 [agency] 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 role of the Chief Audit Executive [and, where the internal audit function uses an outsourced service delivery model, the external service provider] will be approved by the [Accountable Authority] 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. The results of the reviews will be reported to the Audit and Risk Committee who will provide advice to the Accountable Authority on those results.

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 [Accountable Authority] on the recommendation of the Audit and Risk Committee.

Annexure B

Model Audit and Risk Committee Charter

Audit and Risk Committees of NSW agencies are required to have a Charter that is consistent with the content of the 'model charter'. The Accountable Authority and the Audit and Risk Committee are therefore required to review their existing charters against this model. Agencies should consider carefully their particular circumstances, as there may be additional agency specific requirements that shall also be addressed.

The [Accountable Authority] has established the Audit and Risk Committee ('the Committee') in compliance with the *Internal Audit and Risk Management Policy for the General Government Sector.*

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 [Accountable Authority] by monitoring, reviewing and providing advice about the [agency]'s governance processes, risk management and control frameworks and its external accountability obligations.

Authority

The [Accountable Authority] 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 [Accountable Authority], at committee meetings
- obtain external legal or other professional advice, as considered necessary to meet its responsibilities. The payment of costs for that advice by the agency is subject to the prior approval of the Accountable Authority.

Composition and tenure

The Committee will consist of at least three (3) members, and no more than five (5) members,[47] appointed by the [Accountable Authority].

The [Accountable Authority] will appoint the chair and members of the Committee. The chair is counted as one member of the Committee.

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

The chair shall be appointed for one (1) term only for a period of at least three (3) years, with a maximum period of five (5) years. The term of appointment for the chair can be extended but any extension shall

[47] Inclusive of the Chair.

not cause the total term to exceed five (5) years as a chair of the Audit and Risk Committee. Current employees of all NSW government sector agencies[48] other than State Owned Corporations cannot serve as members or chairs of an Audit and Risk Committee.

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

Roles and responsibilities

The Committee has no executive powers.

The Committee is directly responsible and accountable to the [Accountable Authority] for the exercise of its responsibilities. In carrying out its responsibilities, the Committee shall at all times recognise that primary responsibility for management of the [agency] rests with the [Accountable Authority].

The responsibilities of the Committee may be revised or expanded in consultation with, or as requested by, the [Accountable Authority] from time to time.

The Committee's responsibilities are to:

Risk management

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

External accountability

- assess the policies and procedures for management review and consideration of the financial position and performance of the agency including the frequency and nature of that review (including the approach taken to addressing variances and budget risks)
- review procedures around early close and year-end
- review the financial statements and provide advice to the [Accountable Authority] (including whether appropriate action has been taken in response to audit recommendations and adjustments) and recommend their signing by the [Accountable Authority]

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

- satisfy itself that the financial statements are supported by appropriate management signoff on the statements
- review the Chief Financial Officer Letter of Certification and supporting documentation (consistent with Treasury Policy Certifying the Effectiveness of Internal Controls Over Financial Information (TPP17-06))
- review cash management policies and procedures
- review policies and procedures for collection, management and disbursement of grants and tied funding
- review the processes in place designed to ensure that financial information included in the [agency]'s annual report is consistent with the signed financial statements
- satisfy itself that the [agency] appropriately measures and reports on its performance against objectives and State Outcomes.[49]

Compliance and ethics

- determine whether management has appropriately considered legal and compliance risks as part of the [agency]'s risk assessment and management arrangements
- review the effectiveness of the system for monitoring the [agency]'s compliance with applicable laws, regulations and associated government policies
- seek assurance that the appropriate exercise of delegations is monitored and reviewed
- seek assurance that changes in key laws, regulations, internal policies and Accounting Standards affecting the agency's operations are being monitored at least once a year, and appropriately addressed
- review the agency's process for communicating the code of conduct to staff and seek assurance as to compliance with the code
- review policies and processes for identifying, analysing and addressing complaints
- review whether management has taken steps to embed a culture which is committed to ethical and lawful behaviour.

Internal audit

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

[49] This includes consideration of Outcomes Budgeting measures such as Outcome Indicators and Program Performance Measures.

External audit

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

Responsibilities of members

Members of the Committee are expected to understand and observe the requirements of the Internal Audit and Risk Management Policy. Members are also expected to:

- make themselves available as required to attend and participate in meetings
- contribute the time needed to study and understand the papers provided
- apply good analytical skills, objectivity and good judgement
- abide by the relevant ethical codes that apply to employment within the General Government Sector
- express opinions frankly, ask questions that go to the fundamental core of the issue and pursue independent lines of enquiry.

Reporting

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

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

The Committee may, at any time, report to the [Accountable Authority] 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 [Accountable Authority].

Reporting Lines

The Committee shall 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 [Accountable Authority] on functional matters.

The following reporting line is prescribed where the dotted line represents the 'administrative' reporting line and the bold line represents the 'functional' reporting line:

*Note: Internal audit is responsible for providing assurance to the Accountable Authority and the Audit and Risk Committee on the effectiveness of the risk management framework. However, all agencies are encouraged to nominate a CRO who is responsible for the oversight and promotion of risk management within the agency, designing the agency's risk management framework and for the day-to-day activities of embedding the framework in the agency. The CRO or risk management function should report to either the Accountable Authority or a direct report to the Accountable Authority, such as a member of the executive with responsibility for governance or planning, so that independence of risk management from line management is maintained.

Administrative arrangements

Meetings

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

The chair is required to call a meeting if requested to do so by the [Accountable Authority], or another Committee member.

A meeting plan, including the meeting dates and agenda items, will be agreed by the Committee and [agency] at the beginning of each financial year. The estimated total remuneration per Independent Chair and Member will be determined based on the estimated number of meetings and monitored by the agency. The meeting plan will cover all 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 shall include at least two (2) independent members.

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

The Accountable Authority may attend the meetings of the Audit and Risk Committee. Committee members, if necessary, are able to have in-camera discussions. The Chief Audit Executive, CRO (as relevant), external audit representatives and any other agency representatives may attend Committee meetings, except where the Committee members wish to have in-camera discussions. The Committee may also request the Chief Financial Officer or other employees attend committee meetings or participate for certain agenda items.

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

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

Dispute Resolution

Members of the Committee and the [agency]'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 [Accountable Authority], the chair may, as a last resort, refer the matter to Treasury to be dealt with independently.

Secretariat

The [Accountable Authority] 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 shall 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 [Accountable Authority] stating they do not have any conflicts of interest that would preclude them from being members of the Committee.

Committee members shall 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 an actual, or perceived, conflict of interest, the Chair (or a quorum of the Committee if the conflict of interest arises from the Chair) may excuse them from Committee deliberations on the issue where a conflict of interest exists.

Induction

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

Assessment arrangements

The [Accountable Authority], 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 [Accountable Authority]) with appropriate input sought from the [Accountable Authority], the internal and external auditors, the Chief Risk Officer (as relevant), management and any other relevant stakeholders, as determined by the [Accountable Authority].

Review of charter

At least once a year the Committee will review this Charter. This review will include consultation with the [Accountable Authority].

Any substantive changes to this Charter will be recommended by the Committee and formally approved by the [Accountable Authority].

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

_____

Reviewed by [Accountable Authority] or in accordance with a resolution of the Governing Board of the Statutory Body (Sign and Date)

_____

Annexure C

Internal Audit and Risk Management Policy Attestation Statement Template

The *Internal Audit and Risk Management Policy for the General Government Sector* requires Accountable Authorities to attest to compliance with the 'Core Requirements' set out in the Policy annually. The Accountable Authority shall publish the Attestation Statement in the agency's Annual Report, adjacent to the existing requirement[50] to disclose 'risk management and insurance activities'.

A copy of the Attestation Statement for the prior reporting period shall be forwarded to Treasury on or before 31 October each year. Submissions to Treasury should be emailed to finpol@treasury.nsw.gov.au and addressed to the Director, Financial Management Policy.

The Accountable Authority shall use the below Attestation Statement Template to attest that for the relevant reporting period the agency was either 'compliant', 'non-compliant' or 'in transition' in relation to each of the 'Core Requirements'.

Meaning of 'compliant', 'non-compliant', or 'in transition'

For the purpose of the Policy, **'compliant'** means that the agency has implemented and maintained practices consistent with the Core Requirement(s) of the Policy, for the whole of the financial year.

'Non-compliant' means when the agency has not been compliant with a Core Requirement(s) or Mandatory Requirement(s) of the Policy during the reporting period. Where a compliance breach occurs, agencies are required to follow the Ministerial Exemption Process and shall apply to the agency's Responsible Minister for a Ministerial Exemption from the Core Requirement(s). A copy of the Ministerial Determination shall be attached to this Attestation Statement and sent to Treasury.[51]

An agency may mark **'in transition'** on their Attestation Statement where the agency is in the process of transitioning its arrangements to meet new or changed requirements in the Policy for which transitional arrangements have been provided. Ministerial approval is not required for Core Requirements marked as 'in transition'.

Attesting for Controlled Entities

Where an agency has 'control' of an entity (or subsidiary), as defined in Australian Accounting Standards, the parent agency should include the controlled entities (or subsidiary) in the Attestation Statement except where that entity is required to produce its own annual report. Where a controlled entity (or subsidiary) is scheduled under annual reporting legislation to prepare an annual report, the controlled entity (or subsidiary) shall make its own Attestation.

---

50 Refer *Annual Reports (Departments) Regulation 2015* and *Annual Reports (Statutory Bodies) Regulation 2015*.

51 The Ministerial Determination attached to the Attestation Statement provided to Treasury does not need to be published in the agency's annual report.

Internal Audit and Risk Management Attestation Statement for the 20XX-20XX Financial Year for [agency]

I, [Accountable Authority] am of the opinion that the [agency] has internal audit and risk management processes in operation that are, excluding the exemptions or transitional arrangements described below, compliant with the seven (7) Core Requirements set out in the *Internal Audit and Risk Management Policy for the General Government Sector*, specifically:

Core Requirements		For each requirement, please specify whether compliant, non-compliant, or in transition[52]
Risk Management Framework		
1.1	The Accountable Authority shall accept ultimate responsibility and accountability for risk management in the agency.	
1.2	The Accountable Authority shall establish and maintain a risk management framework that is appropriate for the agency. The Accountable Authority shall ensure the framework is consistent with AS ISO 31000:2018.	
Internal Audit Function		
2.1	The Accountable Authority shall establish and maintain an internal audit function that is appropriate for the agency and fit for purpose.	
2.2	The Accountable Authority shall ensure the internal audit function operates consistent with the International Standards for Professional Practice for Internal Auditing.	
2.3	The Accountable Authority shall ensure the agency has an Internal Audit Charter that is consistent with the content of the 'model charter'.	
Audit and Risk Committee		
3.1	The Accountable Authority shall establish and maintain efficient and effective arrangements for independent Audit and Risk Committee oversight to provide advice and guidance to the Accountable Authority on the agency's governance processes, risk management and control frameworks, and its external accountability obligations.	
3.2	The Accountable Authority shall ensure the Audit and Risk Committee has a Charter that is consistent with the content of the 'model charter'.	

Membership

The independent chair and members of the Audit and Risk Committee are[53]:

- Independent Chair, Name, Start term date, finish term date
- Independent Member 1, Name, Start term date, finish term date
- Independent Member 2, Name, Start term date, finish term date
- [Independent Member 3, Name, Start term date, finish term date]
- [Independent Member 4, Name, Start term date, finish term date].

Shared Arrangements *(delete section if not applicable)*

I, [Accountable Authority] advise that [agency] has entered into an approved shared arrangement with the following Department/agencies:

- [list participating Department/agencies].

[52] Where an agency notes that it has been 'non-compliant' or 'in transition', the Accountable Authority shall complete the 'Departure from Core Requirements' section below.

[53] This should include all Independent Chairs and Members that were on the Audit and Risk Committee for the reporting period and their term. All members of the Audit and Risk Committee shall be independent.

The resources shared include [the Audit and Risk Committee, the Chief Audit Executive and/or the internal audit functions]. The shared Audit and Risk Committee is a [Principal Department Led/Collaborative] Shared Audit and Risk Committee.

Departures from Core Requirements *(delete section if not applicable)*

I, [Accountable Authority] advise that the internal audit and risk management processes for [agency] depart from the following Core Requirements set out in the *Internal Audit and Risk Management Policy for the General Government Sector:*

1. The departure from the Core Requirements is due to the agency implementing measures to achieve compliance with new policy requirements consistent with the permitted transitional arrangements, OR

2. The circumstances giving rise to these departures have been determined by the Responsible Minister and the [agency] has implemented [or is implementing] the following practicable alternative measures to meet the Core Requirements:[54]

Departure	**Reason for departure and description of practicable alternative measures implemented/being implemented**
Non-Compliance	
▪ Core Requirement X	▪ Detailed description of circumstances giving rise to departure(s) ▪ Detailed description of the practicable alternative measures implemented / being implemented to achieve equivalent level of assurance
In Transition	
▪ Core Requirement X	▪ Detailed description of the steps being taken to achieve compliance

These processes, including the practicable alternative measures [being] implemented, demonstrate that the [agency] has established and maintained frameworks, including systems, processes and procedures for appropriately managing audit and risk within the [agency].

[Accountable Authority] or in accordance with a resolution of the Governing Board of the Statutory Body
(Sign and Date)

[Agency Contact Officer]
(Role and contact details)

[54] A copy of the relevant Ministerial Determination which supports the agency's departure from one or more of the Core Requirements **shall** be included with the Attestation Statement.

Annexure D

Ministerial Determination Template

[Agency] compliance with the Internal Audit and Risk Management Policy for the General Government Sector

I, [Responsible Minister] am of the opinion that [agency] has internal audit and risk management processes in operation that are, excluding the exemptions described below, compliant with the Core Requirements set out in the *Internal Audit and Risk Management Policy for the General Government Sector*.

I, [Responsible Minister] understand that the following Core Requirements of *Internal Audit and Risk Management Policy* (TPP20-08) have not been met:

Core Requirement	Reason for non-compliance with the Core Requirement

I note that the following alternative arrangements have been implemented to achieve outcomes equivalent to the requirement(s):

Summary of alternative arrangements	How the alternative arrangements will achieve equivalent outcomes

I, [Responsible Minister] am of the opinion that the practicable alternative measures implemented demonstrate that the [agency] has established and maintained frameworks, including systems, processes and procedures for appropriately managing audit and risk within the [agency].

This exemption to the Core Requirements of the *Internal Audit and Risk Management Policy for the General Government Sector (TPP20-08)* is valid for the financial year(s) (20XX-20XX).[55]

_____

[Responsible Minister]

(Sign and Date)

_____

[Agency Contact Officer]

(Role and contact details)

[55] Exemptions may be sought for a maximum of two financial years.

Annexure E

Small Agency Exemption

The Small Agency Exemption is available when an agency does not fully comply with the Core Requirement(s) during a reporting period and meets all the below eligibility criteria. The Accountable Authority of an agency may apply to Treasury for an ongoing Small Agency Exemption from the requirement to:

a. comply with one or more of the Core Requirements;
b. attest compliance, and/or
c. include the Attestation Statement in the agency's annual reporting information

if:

i. the agency satisfies each of the eligibility criteria below, and
ii. the Responsible Minister of the agency approves the application for an exemption, and
iii. Treasury, as delegated authority of the Treasurer, provides final approval.

This exemption is intended for small, immaterial agencies where the cost of complying with the Core Requirement(s) are not commensurate with the size and risk profile of the agencies.

Any Small Agency Exemptions granted by Treasury prior to the commencement of the Policy will continue to remain in force under the provisions of this Policy.

i. Eligibility Criteria

Agencies may apply to Treasury for a Small Agency Exemption if the agency meets all of the following criteria:

- does not collect taxes on behalf of the NSW Government
- does not receive a direct appropriation from the Consolidated Fund
- is not controlled by an agency required to comply with the Policy
- is an agency considered by Treasury to be immaterial
- does not have annual revenue or expenditure exceeding $15m
- does not have financial assets exceeding $15m
- does not have liabilities exceeding $15m (unless the nature of the liabilities are such that complying with the Policy is deemed not to be required)
- is not a fund manager responsible for the administration and/or management of public monies
- has a risk register that indicates that their risks have been properly identified and that proper measures are in place and being monitored to manage those risks, and
- does not have a risk profile that would warrant full compliance with the Core Requirement(s).

ii. Responsible Minister grants approval for exemption

The Accountable Authority shall first obtain written approval from the Responsible Minister to apply for the Small Agency Exemption. An Accountable Authority's request to the Responsible Minister for such approval shall:

- include evidence that the agency meets all the eligibility criteria, and
- outline the reasons the agency should be exempt from the relevant Core Requirement(s).

iii. Application to Treasury for approval of exemption

Once the approval is obtained, the Accountable authority shall apply to Treasury for the Small Agency Exemption using the template in Annexure F. The application letter shall include:

- A copy of the Responsible Minister's written approval of the agency's application for a Small Agency Exemption
- Written evidence demonstrating how the agency meets each of the above eligibility criteria
- A copy of the most recent annual report of the agency or the audited financial statements for the agency
- A copy of the agency's organisational risk register including a summary of major risks faced by the agency, together with risk treatment strategies adopted by the agency to manage those risks.

Letters should be emailed to finpol@treasury.nsw.gov.au and addressed to the Director, Financial Management Policy.

Assessment Criteria

The application documents received from the agency will be assessed to confirm that:

- the Responsible Minister has approved the application, and
- the agency has met the above eligibility criteria.

Exemption Review Process

Upon notification of the successful grant of a Small Agency Exemption, the exemption will remain in force until any of the following circumstances occur:

- Any major changes to the agency's structure
- The agency receives a direct appropriation
- The agency's revenues include taxes
- The agency's revenues, expenses or liabilities individually increase by more than 20% from the baseline totals/balances indicated in the audited financial statements used for the purposes of assessing the application
- The agency's risk profile materially changes.

The Accountable Authority for an agency with an approved Small Agency Exemption shall consider whether the agency has met any of the above circumstances as at 31 March annually and notify Treasury of any changes no later than 30 April. Upon receipt of such a notification, the information will be reviewed and the agency will be advised as to whether the Small Agency Exemption remains in force.

Annexure F

Application to seek an exemption from the requirement to comply with the policy, Internal Audit and Risk Management Policy for the General Government Sector (TPP20-08)

I, [Accountable Authority] submit this application to Treasury to seek an exemption from the requirements of TPP20-08 Internal Audit and Risk Management Policy for the General Government Sector.

In support of the application, I, [Accountable Authority or governing board of the agency], provide documentary evidence of the Responsible Minister's determination and submit this determination to Treasury as an attachment to the request for an exemption.

I attach evidence, which shows that [agency name] meets each of the eligibility criteria.

I [Accountable Authority or governing board of the agency], attach the Annual Report of the [agency name], including the Audited Financial Statements of the [agency name] for the year ended 30 June 20[XX] comprising of:

- Independent Auditor's Report
- Statement of Comprehensive Income
- Statement of Financial Position
- Statement of Changes in Equity
- Statement of Cash Flows
- Notes to the financial statements.

I [Accountable Authority or governing board of the agency] attach a summary of the major risks faced and risk treatment strategies adopted by [agency name] to manage its risks.

_____

[Accountable Authority] or in accordance with a resolution of the Governing Board, on behalf of the Statutory Body
(Sign and Date)

_____

[Agency Contact Officer]
(Role and contact details)

Annexure G

Shared Arrangements

The aim of Shared Arrangements is to ensure that the compliance cost of implementing the Core Requirements for agencies is proportionate to their benefit and commensurate with their risk profile. Shared Arrangements may be formed between agencies to support Accountable Authorities with implementing the Core Requirements in an efficient and effective manner.

The resources that may be shared to achieve efficiencies include sharing the cost of the:

A. ARC (engaging independent ARC members and Chair and secretariat services), and/or
B. CAE, and/or
C. Internal Audit Function.

Regardless of the form of a Shared Arrangement, approval by the Cluster Secretary of Shared Arrangements does not diminish each Accountable Authority's responsibility to meet their obligations under s 3.6 of the GSF Act. This includes ensuring efficient and effective independent advice and oversight continues to be provided to each Accountable Authority, and CAEs and/or Internal Audit Functions have the capacity to operate effectively.

The below explains variations to Core Requirements 2.1, 3.1 and 3.2 for Shared Arrangements.

Requirements of a Shared Arrangement

Accountable Authorities may enter their agency into a shared arrangement if the:

- Requirements of a Principal Department Led or Collaborative Shared ARC are met, if applicable (refer to A. Shared Audit and Risk Committees below), and/or
- Requirements of sharing a CAE and/or Internal Audit function are met, if applicable (refer to B. Shared CAE or Internal Audit function below), and
- Shared Arrangements Agreement is signed by all Accountable Authorities in the Shared Arrangement, and
- Cluster Secretary approves the Shared Arrangement.

Shared Arrangement Agreement

All agencies entering into a shared arrangement shall agree and sign a Shared Arrangement Agreement. There is no prescribed format for an agreement, which should be drawn up to suit the needs of the participating agencies. However, the following key aspects should be included in a Shared Arrangement Agreement:

General

- clearly set out the terms of the arrangement including details of the shared ARC and if applicable, shared CAE and internal audit functions
- state the role and responsibilities of each agency
- be signed by all Accountable Authorities
- be approved by the Cluster Secretary

Where it is proposed to share a CAE

- specify the functional and administrative reporting lines of the CAE
- include the authority of the CAE to request and receive information from all agencies within the shared arrangement

Where it is proposed to share an ARC

- detail clear reporting lines to ensure that all participating agencies understand the objectives and responsibilities of the shared ARC to report and provide independent advice and oversight for each participating agency in the shared arrangement
- provide for shared secretariat services (including minuting, distribution and reporting packs).

Other provisions that should be considered in the agreement include:

- how costs will be administered and shared
- how the committee members will be appointed and reviewed
- remuneration arrangements for committee members and cost sharing arrangements
- what information, if any, is to be shared between agencies and how
- parameters on sharing key audit and risk issues between agencies within the cluster (e.g. CAE's regularly communicating with agencies in other ARC arrangements within their cluster)
- how information is to be provided to the CAE
- how information is to be provided to the Secretariat
- meeting schedule, including sequencing of meetings to cover each agency's business and agency representatives as required (e.g. Accountable Authority, CFO and CAE)
- how the internal audit function is to be delivered and, where an outsourced delivery model is adopted, the title of the position who is to be the in-house liaison/contract officer in each agency (if applicable)
- who is responsible for ensuring the ARC charter is reviewed in accordance with this Policy
- the mechanism for formulating and delivering the annual report on the ARC's performance and for managing the ARC's performance. Input from the Accountable Authorities of all participating agencies should be considered in this performance review
- the Secretariat will be the custodian of all documentation relating to the Shared Arrangement Agreement.

A. Shared Audit and Risk Committees

Under Core Requirement 3.1, the Accountable Authority of each agency is responsible for establishing efficient and effective arrangements for ARC oversight to oversee and monitor governance, risk and control issues affecting the operations of the agency. A shared ARC can be an efficient and effective means of providing ARC oversight for a number of agencies. At a cluster level, a shared ARC can leverage cost efficiencies in operating ARCs, group agencies with common functions to share the specialist skills of ARC members and improve communication between entities within the cluster.

For each cluster, the Cluster Secretary can support this by ensuring efficient and effective oversight arrangements are established within their cluster and sufficient advice and guidance is provided to each agency's Accountable Authority. The Cluster Secretary should consult with each Accountable Authority (except agencies defined as Special Offices) in their cluster to:

a) first consider whether an agency may enter into a Principal Department Led Shared ARC, or

b) if specific circumstances are met, consider forming a Collaborative Shared ARC or standalone ARC.

   Specific circumstances where it may be more appropriate to form a collaborative shared ARC or a standalone ARC (rather than a Principal Department led ARC) include:

   - All Requirements of a Principal Department Led ARC cannot be met
   - Agency is a Special Office
   - Agency has a role that requires independence from other agencies
   - Agency's risk profile warrants stand-alone arrangements
   - Secrecy provisions applicable to an agency could be breached if they enter a shared arrangement.

All agencies are encouraged to share key audit and risk issues with other agencies in their cluster. Regardless of which type of ARC arrangement an agency has, the sharing of information should be facilitated throughout each cluster where possible. This may include CAEs regularly communicating with the Department and agencies in other ARC arrangements within their cluster.

As mentioned above, there are two forms of Shared ARC Arrangements:

- Principal Department Led Shared ARC, or
- Collaborative Shared ARC.

Regardless of the form of arrangement, a shared ARC will operate as an individual ARC for each separate agency. This requires members of the ARC to liaise with the respective Accountable Authority, ensure separate records and confidentiality are maintained, and provide independent advice and oversight for each participating agency.

Clusters may establish any combination of ARC arrangements suitable to their risk profile and structure. Figure 5 below is an example of how a cluster may utilise a combination of ARCs.

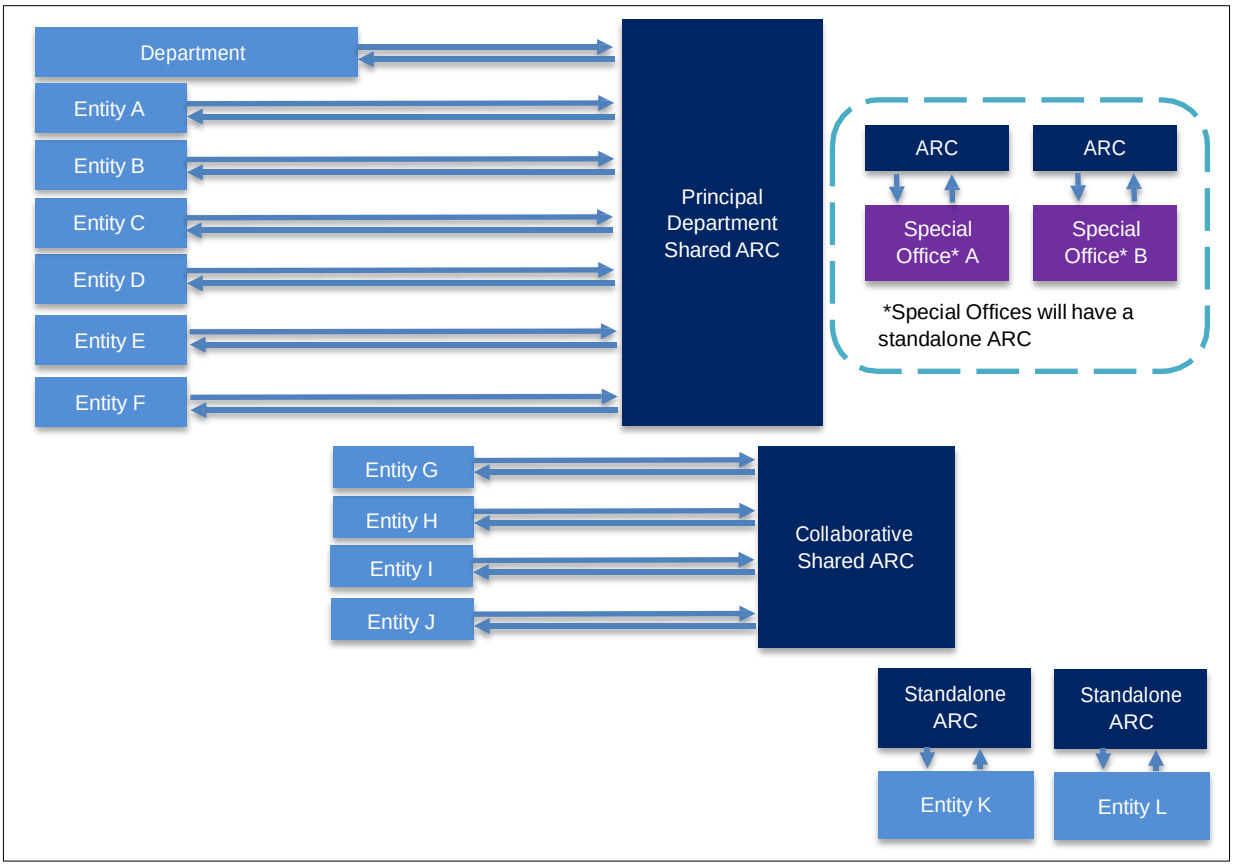


Figure 5: Example of a cluster's combination of ARC arrangements

Principal Department Led Shared ARC

In this model, the independent Chair and members of the Department's ARC extend their oversight to additional agencies within the cluster. The Principal Department led ARC provides independent advice and oversight to each Accountable Authority in the shared ARC and to the Cluster Secretary. The Principal Department defines the roles and responsibilities of participating agencies and appoints the ARC members, chair and secretariat.

The Cluster Secretary should ensure efficient and effective oversight arrangements are established within their cluster and sufficient advice and guidance is provided to each agency's Accountable

Authority. This is achieved by ensuring the below requirements of a Principal Department Led ARC are followed.

Requirements of a Principal Department Led ARC

- Accountable Authority for each participating agency agrees to participate in the shared ARC
- The independent ARC chair and members have the time and capacity to sufficiently cover all agencies in the ARC
- The shared ARC maintains an appropriate level of visibility of each of the agency's operations and reporting relationship with each Accountable Authority
- Accountable Authority for each agency has direct access to the ARC
- Accountable Authority for each agency shall ensure the secrecy provisions applicable to their agency are not breached if they enter the shared ARC
- Any participating agency is not a Special Office
- The risk profile of any participating agency does not warrant stand-alone arrangements
- Any participating agency does not have a role that requires independence from other agencies
- The ARC covers each agency's business separately in sequential meetings and not joint sittings (refer to the Sequential Meeting Requirements listed below)
- The ARC composition includes a sufficient number of independent members to provide adequate coverage over the agencies but a maximum of 5 ARC members, inclusive of the chair, remains the same as Core Requirement 3.1
- Shared ARC arrangements are detailed in the Shared Arrangement Agreement signed by the Accountable Authorities of all participating agencies and shall include a dispute resolution process
- The ARC has a shared ARC Charter which aligns with the model ARC Charter in this Policy (refer to Annexure H and I)
    - The Charter shall outline the purpose, authority and scope of responsibility and be adapted to overseeing more than one agency
    - The Charter shall be reviewed annually by the ARC Chair in consultation with all of the Accountable Authorities in the shared arrangement
- Independent chairs and members are appointed in accordance with the Prequalification Scheme Guidelines and Conditions including remuneration
- The Cluster Secretary shall approve all shared arrangements including shared ARCs
- Unless provided for in this Shared Arrangements section, compliance is required with all other Core Requirements in this Policy including the ARC composition, code of conduct of members and chairs and annual attestation.
- *Specific to Principal Department Led ARC:*
    - Principal Department's Accountable Authority is responsible for:
        - annually reviewing the performance of the ARC Chair and members, and
        - providing formal feedback to the Chair of the ARC.
- *Sequential Meeting Requirements:*
  The oversight role of an ARC is to provide advice and guidance to the Accountable Authority on the agency's governance processes, risk management and control frameworks, and its external accountability obligations. Regardless of the form of arrangement, a shared ARC will operate as an individual ARC for each separate agency and provide independent advice and oversight for each participating agency. Therefore, this requires ARC meetings to be held sequentially for each agency in the shared ARC. This includes:
    - Meeting schedule allocating time for each agency and for relevant agency representatives
    - Covering each agency's business separately
    - Depending on the size and complexity of the ARC, sequential meetings may spread over two or more meeting days if required to sufficiently cover all agencies in the ARC. A typical meeting day is a normal business day with time allocated for each agency
    - Each participating agency may contribute to agenda setting

- Shared Arrangement Agreement includes ability for Accountable Authorities and agency representatives, if necessary, to have in-camera discussions with the ARC
- Cluster representatives (including the Accountable Authority, Chief Financial Officers, Senior Accounting Officers, CROs and CAEs) may attend the ARC meetings for all agencies within their shared arrangement at the invitation of the Chair and with the consent of all participating agencies
- External audit representatives may consider that discussing individual agency matters at ARC meetings when cluster representatives are present is incompatible with the secrecy provisions in section 38 of the *Public Finance and Audit Act 1983* and their professional membership obligations. Where this is the case, the external audit representatives may seek to discuss matters with the ARC and relevant agency through in camera sessions
- External audit representatives may request in camera sessions with the ARC (and relevant agency representatives if required)
- Sequential meetings may involve the meetings being formally closed, a separate agenda and separate minutes for each agency. If different arrangements for sequential meetings are established, the Accountable Authority for each agency shall ensure the secrecy provisions applicable to their agency are not breached and each agency is allocated sufficient time to ensure adequate and dedicated ARC coverage.

Collaborative Shared ARC

In this model, the Accountable Authority of each agency in the shared ARC negotiates and agrees on the administrative and resource sharing arrangements. Each agency has equal standing to decide on the ARC arrangements. The Collaborative Shared ARC provides independent advice and oversight to each Accountable Authority in the shared ARC.

Collaborative Shared ARCs are particularly suitable for agencies within the cluster that:

- share a common aim or organisational values, and/or
- deliver on similar service delivery obligations, and/or
- regularly collaborate to provide joint services.

Accountable Authorities of agencies in a Collaborative Shared ARC shall ensure the following requirements are followed:

- Meet all the Requirements of a Principal Department Led ARC above (except those indicated as specific to a Principal Department Led ARC), and
- All Accountable Authorities for agencies in the shared ARC negotiate and agree on the terms of the Shared Arrangement Agreement including:
  - roles and responsibilities of participating agencies
  - appointing one of the Accountable Authorities in the shared arrangement to be responsible for appointing the ARC members and chair, and
  - appointing a joint secretariat.
- For the annual performance review of a Collaborative Shared ARC, the Accountable Authorities of each agency are responsible for ensuring it is performed annually and feedback is provided to the ARC Chair. Agencies may collaborate in developing a performance evaluation mechanism which may include, if all agencies agree, a consolidated report rather than separate reports. The agreed mechanism should be included in the Shared Arrangement Agreement including who will be responsible for taking appropriate action where necessary.
- When including the dispute resolution process in the Shared Arrangement Agreement, it should include that all agencies are required to monitor the operation of the agreement and hold one another accountable.

Further information is provided below on the types of shared ARCs.

B. Shared CAE and internal audit functions

An agency may agree to share a CAE and/or internal audit function, unless:

- The agency is a Special Office
- The agency has a role that requires independence from other agencies
- Secrecy provisions applicable to the agency could be breached if they enter a shared arrangement
- The complexity and diversity in the business of the agency is such that a CAE and/or internal audit function shared with other agencies will not be able to attain an adequate level of understanding of all relevant issues
- There is a possibility of a substantive actual or perceived conflict of interest to arise in a shared arrangement.

The decision to share a CAE and/or Internal Audit Function is independent from the decision to share an ARC. There may be some instances where it is not appropriate for an agency to share a CAE and/or Internal Audit Function but still be able to enter a Shared Arrangement for an ARC (subject to the above requirements relating to Shared Audit and Risk Committees being met).

When reviewing a proposal to share a CAE and/or Internal Audit Function, the Cluster Secretary is to consider the likely demands on the CAE and/or Internal Audit Function as a result of the Shared Arrangement. This should include the CAE and/or Internal Audit Function having the capacity to understand the different business activities of multiple agencies and manage the larger workload. The Cluster Secretary may consult with applicable ARCs on this matter.

A Shared Internal Audit Function may be in-house, outsourced or co-sourced but the role of the CAE cannot be outsourced to an independent party. The CAE will be:

- in the case of a Principal Department Led Shared Arrangement, an employee of the principal department, or
- in the case of a Collaborative Shared Arrangement, an employee of one of the participating agencies (as agreed by the Accountable Authorities of each of the participating agencies).

The appointment of a CAE will be approved by the Accountable Authority of the employer agency. Appointments should take into account the complexities raised by the Shared Arrangement and due consideration made to appointing a CAE who is appropriately qualified and/or experienced. All CAE appointments shall be made in consultation with the members of all applicable ARCs for agencies in which the CAE will be providing services. Where the CAE is shared, the CAE will assume the responsibilities of a CAE stated in the Core Requirements of this Policy on behalf of all agencies in the Shared Arrangement (except where an agency chooses to have an independent CAE). Where an agency is participating in a Shared ARC Arrangement but wishes to have an independent CAE, the CAE shall be appointed from within that agency and in consultation with the members of the shared ARC.

The reporting lines of the CAE will accord with the requirements of this Policy. In the case of a shared ARC, the CAE will report **functionally** to the shared ARC.[56] In the case of a Principal Department Led Shared Arrangement, the CAE will report **administratively** to the Cluster Secretary or a Senior Executive level direct report of a Cluster Secretary. In the case of a Collaborative Shared Arrangement, the CAE will report to the Accountable Authority of one of the agencies entering into the Shared Arrangement or Senior Executive level direct report of that Accountable Authority. The operational independence of a CAE shall be paramount and the requirements of 2.1.14 in this Policy should be applied to arrangements to share a CAE to ensure this. The Shared Arrangement Agreement should clearly specify the reporting relationships of the CAE.

[56] Further guidance on the reporting relationships of the CAE can be found at 2.1.14 of this Policy.

Each agency entering into an arrangement for a shared CAE should nominate a person within their organisation to be responsible for liaising with the CAE.

Where a Shared Arrangement has been established for an Internal Audit Function, an Internal Audit Charter, consistent with the Model Internal Audit Charter at Annexure A should be prepared in consultation with all applicable ARCs and endorsed by the Accountable Authority of each participating agency. The reporting relationships of the CAE(s) in a Shared Arrangement (even in those cases where one or more agencies in the Shared Arrangement have their own CAE) should be outlined in the Charter.

Application process for a Shared Arrangement

It is the responsibility of the Accountable Authority for each agency to decide the appropriate assurance arrangements for their agency including whether to enter a shared arrangement.

Where the Accountable Authorities in a cluster:

- have identified an opportunity to enter into a shared arrangement,
- are satisfied that their agencies meet the above requirements of a shared arrangement, and
- have agreed to pursue a shared arrangement (i.e. Principal Department Led or Collaborative ARC and/or the sharing of a CAE and/or internal audit functions),

they shall jointly address a letter seeking approval for a shared arrangement to their Cluster Secretary.

The letter should:

- identify the agencies proposing to enter into a shared arrangement
- include a brief description of the proposed arrangement including resources to be shared (ARC and/or CAE and/or internal audit functions) and how specific Core Requirements will be varied under equivalent alternative shared arrangements (refer to the Variations to the Core Requirements table below for examples)
- address how each of the Requirements of a Principal Department Led or Collaborative shared ARC arrangement are met
- address, if applicable, how each of the requirements of sharing a CAE and/or Internal Audit function are met and details of which agency will provide the shared CAE and/or internal audit function
- Include the proposed Shared Arrangement Agreement to be signed by the Accountable Authorities of all participating agencies
- Include the Shared Audit and Risk Committee Charter
- Include, if applicable, the Internal Audit Charter.

Once approved, a copy of the letter, accompanying documents and approval documentation shall be provided to Treasury.

Documents to be provided to Treasury should be emailed to finpol@treasury.nsw.gov.au and addressed to the Director, Financial Management Policy.

The above application process is repeated if there is a change to a previously approved shared arrangement (e.g. an additional agency is added to a shared ARC).

The Cluster Secretary's approval of a shared arrangement in accordance with the above requirements, and the participating agencies' compliance with the Shared Arrangement Agreement's terms, constitutes compliance with the relevant Core Requirements in this Policy. Details of the shared arrangement shall be included in the annual attestation. Refer to the Requirements for an Attestation Statement section for further details.

For the avoidance of doubt, an exemption to this Policy is not required if a Shared Arrangement is approved by the Cluster Secretary. Unless provided for in this section and by an approved Shared Arrangement, all other Core Requirements in this Policy shall be followed.

Variations to the Core Requirements

Refer to the examples below of variations to Core Requirements 2.1, 3.1 and 3.2 for Shared Arrangements:

	Clause(s)	Core Requirement	Equivalent Shared arrangement
1	2.1.7	CAE should be appointed from within the agency by the Accountable Authority	Where a CAE role is to be shared, the Accountable Authorities entering in a shared arrangement should agree for a CAE to be appointed from one of the agencies entering into the shared arrangement (in the case of a Principal Department Led arrangement, this will be the Principal Department CAE). The details should be set out in a Shared Arrangement Agreement and briefly described in the application.
2	2.1.9	The Accountable Authority shall consult with the ARC in appointing and removing a CAE	The Accountable Authority nominated as responsible for appointing the CAE on behalf of the other agencies in the shared arrangement is also responsible for consulting with the ARC in removing a CAE. The arrangement should be briefly described in the application.
3	2.1.14	CAE reports functionally to the ARC and administratively to the Accountable Authority	Where a CAE role is to be shared, the CAE will report administratively to the Accountable Authority of one of the agencies in the shared arrangement (in the case of a Principal Department Led arrangement, the CAE will report administratively to the Principal Department's Accountable Authority). The details should be set out in a Shared Arrangement Agreement and briefly described in the application. The Internal Audit and ARC charters should be amended to reflect this reporting relationship.
4	3.1.6 3.1.7	The Accountable Authority should appoint the Chair and members of the ARC	In a shared arrangement, one of the Accountable Authorities will be empowered by a Shared Arrangement Agreement to appoint the Chair and ARC members on behalf of all the other agencies participating in the arrangement (in the case of a Principal Department led arrangement, the Principal Department's Accountable Authority will select and appoint the Chair and ARC members). The arrangement should be briefly described in the application.

	Clause(s)	Core Requirement	Equivalent Shared arrangement
5	3.2.21	The Accountable Authority shall establish a mechanism to review and report on the performance of the ARC	In a collaborative shared arrangement, the mechanism and process for reviewing and reporting on the performance of the ARC as a whole, and the performance of the Chair and each member is agreed between the participating agencies. In the case of a Principal Department Led arrangement, the Principal Department Accountable Authority will be responsible for the ARC performance review.

Further guidance on shared arrangements

There are several relevant Core Requirements and terms stated in the Prequalification Scheme Conditions[57] (Scheme Conditions) which are applicable to Shared ARCs and are reiterated below for further guidance:

- Composition guidelines for the ARC will remain the same regardless of the type of shared arrangement including appointing only 'independent members' (including an 'independent chair') to the ARC. Accountable Authorities, Chief Financial Officers, Senior Accounting Officers and CAEs shall not be members of the shared ARC but may attend meetings as observers as determined by the Chair. Independent chairs and members shall be selected from the list of pre-qualified individuals in the Prequalification Scheme.
- ARCs shall meet at least four times per year or more frequently as circumstances dictate. Larger and more complex shared ARCs may require more frequent meetings in order for the ARC to effectively perform its roles and discharge its responsibilities and meetings may extend over several days. Shared ARC meetings are held sequentially, and a quorum will consist of a majority of members.
- Remuneration of the Chair and members of a shared ARC shall be in accordance with the Scheme Conditions, including as prescribed by the fee category table.
- The Scheme Conditions limits the number of committees a pre-qualified independent member can serve on to five (5) committees. Membership of a shared ARC will count as one committee for the purposes of the Scheme Conditions. Members are required to disclose membership of all shared ARCs and sub committees to the operators of the Prequalification Scheme (NSW Procurement, Treasury) and to the Accountable Authority.
- Each agency entering into a shared arrangement is required to provide an attestation to Treasury in accordance with this Policy and make a declaration in their annual report. This attestation will include details of any shared arrangement entered.

Further guidance on the types of shared ARCs

Further information on the differences between the two types are provided below.

Principal Department Led ARC

- The Principal Department Led ARC extends their oversight to additional agencies within their cluster
- The Principal Department articulates the roles and responsibilities of agencies participating in the shared arrangement and those agencies that choose to opt in
- The Principal Department appoints the Secretariat
- The Principal Department selects and appoints the Chair and members

[57] Prequalification Scheme: Audit and Risk Committee Independent Chairs and Members – Conditions – December 2020.

- The Principal Department shall establish a Shared Arrangement Agreement with the participating agencies to formalise the arrangements
- The Principal Department's Accountable Authority is responsible for annually reviewing the performance of the ARC Chair and members, providing formal feedback to the Chair of the ARC and taking appropriate action where necessary. Input from the Accountable Authorities of other participating agencies should be considered in this review. The Principal Department should ensure that the process is documented in the Shared Arrangement Agreement
- The Principal Department should ensure that the process for managing disputes is documented in the Shared Arrangement Agreement.

Collaborative

- The Accountable Authority of each agency in the shared ARC negotiates and agrees to enter into a shared arrangement.
- The Accountable Authorities of all agencies in the shared arrangement agree on the roles and responsibilities of each agency, including a joint secretariat.
- The Accountable Authority of one of the agencies is responsible for engaging the Chair and members through a process agreed upon by all the agencies entering into the shared arrangement.
- The Accountable Authorities of each agency are responsible for ensuring an annual performance review of the ARC is performed and feedback is provided to the ARC Chair. Agencies may collaborate in developing a performance evaluation mechanism which may include, if all agencies agree, a consolidated report rather than separate reports. The Shared Arrangement Agreement should document the performance appraisal process and who will be responsible for taking appropriate action where necessary.
- All agencies are required to monitor the operation of the agreement, hold one another accountable and establish a dispute resolution process as part of the Shared Arrangement Agreement.

Annexure H

Model Audit and Risk Committee Charter (Principal Department Led Shared Arrangement)

Audit and Risk Committees of NSW agencies are required to have a Charter that is consistent with the content of the 'model charter'. This model charter is based on the model charter in Annexure B of this Policy and is for agencies entering into a shared arrangement with a Principal Department Audit and Risk Committee. In doing so it is important that each agency consider carefully its particular circumstances, as there may be additional agency specific requirements that shall also be addressed.

The Principal Department has established an Audit and Risk Committee ('the Committee') in compliance with the *Internal Audit and Risk Management Policy for the General Government Sector*. The following Accountable Authorities have agreed that the Committee will provide oversight for these agencies through a shared arrangement.

Agency	Accountable Authority

For the purposes of this charter these organisations will herein be referred to collectively as "the participating entities".

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 Accountable Authorities of all participating entities by monitoring, reviewing and providing advice about the participating entities' governance processes, risk management and control frameworks, and external accountability obligations.

Authority

The Accountable Authorities of the participating entities authorise 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 Accountable Authorities of the participating entities at committee meetings
- obtain external legal or other professional advice, as considered necessary to meet its responsibilities, at the expense of any or all of the participating entities subject to the approval of the Accountable Authorities of the relevant participating entities.

Composition and tenure

The Committee will consist of at least three (3) members, and no more than five (5) members,[58] appointed by the [Accountable Authority].

The Accountable Authority of [Principal Department] will appoint the chair and members of the Committee. The Chair is counted as one member of the Committee.

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

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

Current employees of all NSW government sector agencies[59] other than State Owned Corporations cannot serve as members or chairs of an Audit and Risk Committee.

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

Roles and responsibilities

The Committee has no executive powers.

The Committee is directly responsible and accountable to each particular Accountable Authority for the exercise of its responsibilities pertaining to that entity. In carrying out its responsibilities, the Committee shall at all times recognise that primary responsibility for management of each participating entity rests with the Accountable Authority of that entity.

The responsibilities of the Committee may be revised or expanded in consultation with, or as requested by, the Accountable Authorities of the participating entities from time to time.

The Committee's responsibilities in regards to each participating entity in the shared arrangement are to:

Risk management

- review whether management has in place a current and appropriate risk management framework that is consistent with *AS ISO 31000:2018*
- assess and advise on the maturity of the agency's risk management framework and risk culture
- consider the adequacy and effectiveness of the internal control and risk management frameworks by reviewing reports from management, internal audit and external audit, and by monitoring management responses and actions to correct any noted deficiencies
- review the impact of the agency's risk management on its control environment and insurance arrangements

[58] Inclusive of the Chair.

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

- review the agency's fraud and corruption control framework including the fraud control plan and be satisfied that the agency has appropriate processes and systems in place to capture and effectively investigate fraud related information
- seek assurance from management that emerging risks (including, but not limited to, climate risk and cyber risk) are being identified and addressed
- seek assurance from management and Internal Audit that risk management processes are operating effectively, including that relevant internal control policies and procedures are in place and that these are periodically reviewed and updated
- review whether a sound and effective approach has been followed in developing risk management plans for major projects, programs or undertakings
- review whether a sound and effective approach has been followed in establishing the agency's business continuity planning arrangements, including whether disaster recovery plans have been tested periodically.
- review the significant risks arising from the strategic and operational activities of each agency that affect, or are likely to affect, other participating agencies in the shared arrangement and seek assurance that risk treatment measures have been developed.

External accountability

- assess the policies and procedures for management review and consideration of the financial position and performance of the agency including the frequency and nature of that review (including the approach taken to addressing variances and budget risks)
- review procedures around early close and year-end
- review the financial statements and provide advice to the [Accountable Authority] (including whether appropriate action has been taken in response to audit recommendations and adjustments) and recommend their signing by the [Accountable Authority]
- satisfy itself that the financial statements are supported by appropriate management signoff on the statements
- review the Chief Financial Officer Letter of Certification and supporting documentation (consistent with Treasury Policy Certifying the Effectiveness of Internal Controls Over Financial Information (TPP17-06))
- review cash management policies and procedures
- review policies and procedures for collection, management and disbursement of grants and tied funding.
- review the processes in place designed to ensure that financial information included in the [agency]'s annual report is consistent with the signed financial statements
- satisfy itself that the [agency] appropriately measures and reports on its performance against objectives and State Outcomes.[60]

Compliance and ethics

- determine whether management has appropriately considered legal and compliance risks as part of the [agency]'s risk assessment and management arrangements
- review the effectiveness of the system for monitoring the [agency]'s compliance with applicable laws, regulations and associated government policies
- seek assurance that the appropriate exercise of delegations is monitored and reviewed
- seek assurance that changes in key laws, regulations, internal policies and Accounting Standards affecting the agency's operations are being monitored at least once a year and appropriately addressed
- review the agency's process for communicating the code of conduct to staff and seek assurance as to compliance with the code
- review policies and processes for identifying, analysing and addressing complaints
- review whether management has taken steps to embed a culture which is committed to ethical and lawful behaviour.

[60] This includes consideration of Outcomes Budgeting measures such as Outcome Indicators and Program Performance Measures.

Internal audit

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

External audit

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

Responsibilities of members

Members of the Committee are expected to understand and observe the requirements of the Internal Audit and Risk Management Policy. Members are also expected to:

- make themselves available as required to attend and participate in meetings
- ensure they have the time and capacity to sufficiently cover all agencies in the shared Audit and Risk Committee including the time needed to study and understand the papers provided
- apply good analytical skills, objectivity and good judgement
- abide by the relevant ethical codes that apply to employment within the General Government Sector
- express opinions frankly, ask questions that go to the fundamental core of the issue and pursue independent lines of enquiry.

Reporting

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

- an overall assessment of the agency's risk, control and compliance framework, including details of any significant emerging risks or legislative changes impacting the agency
- a summary of the work the Committee performed to fully discharge its responsibilities during the preceding year

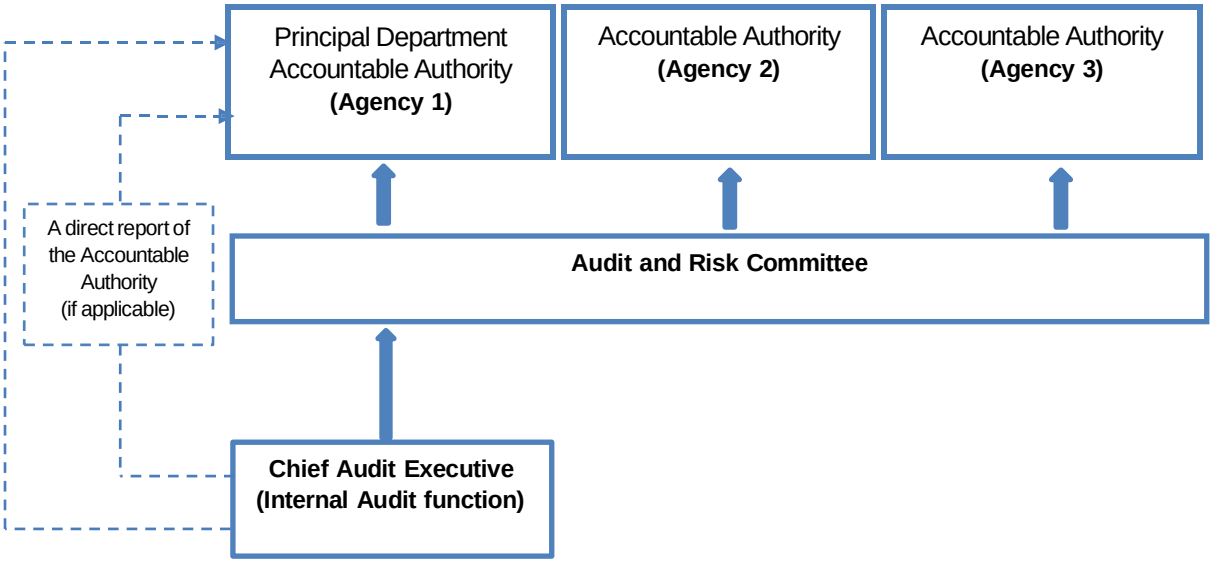
- details of meetings, including the number of meetings held during the relevant period, and the number of meetings each member attended
- a summary of the agency's progress in addressing the findings and recommendations made in internal and external reports
- a summary of the Committee's assessment of the performance of internal audit.

The Committee may, at any time, report to the [Accountable Authority] 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 [Accountable Authority].

Reporting Lines

The Committee shall 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 [Accountable Authority] on functional matters.

The following reporting line is prescribed where the dotted line represents the 'administrative' reporting line and the bold line represents the 'functional' reporting line:



Administrative arrangements

Meetings

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

The Chair is required to call a meeting if requested to do so by any participating entity's Accountable Authority, or another Committee member.

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

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

Attendance at meetings and quorums

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

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

The Accountable Authority of each participating entity may attend the meetings of the Audit and Risk Committee relevant to their agency. Committee members, if necessary, are able to have in-camera discussions. Each participating agency's Chief Audit Executive, Chief Risk Officer (as relevant), external audit representatives and any other agency representatives may attend Committee meetings relevant to their agency, except where the Committee members wish to have in-camera discussions. The Committee may also request the Chief Financial Officer and/or other representatives of participating agencies, and/or the Principal Department, to attend relevant committee meetings or participate for certain agenda items.

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

Dispute Resolution

Members of the Committee and each participating entity'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 Accountable Authorities of participating entities, the Chair may, as a last resort, refer the matter to Treasury to be dealt with independently.

Secretariat

The Principal Department is responsible for appointing a person or persons to act as the Secretariat, and this will be outlined in a Shared Arrangement Agreement. 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 shall 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 Principal Department's Accountable Authority stating they do not have any conflicts of interest that would preclude them from being members of the Committee.

Committee members shall 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 an actual, or perceived, conflict of interest, the Chair (or a quorum of the Committee if the conflict of interest arises from the Chair) may excuse them from Committee deliberations on the issue where a conflict of interest exists.

Induction

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

Assessment arrangements

The Principal Department is responsible for reviewing 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 Principal Department's Accountable Authority) with appropriate input sought from the participating entities' Accountable Authorities, internal and external auditors, CROs (as relevant), management and any other relevant stakeholders, as determined by the Principal Department's Accountable Authority.

Arrangements for review of performance should be documented in the Shared Arrangement Agreement.

Review of charter

At least once a year the Committee will review this Charter. This review will include consultation with the Accountable Authorities of the participating entities in the shared arrangement.

Any substantive changes to this Charter will be recommended by the Committee and formally approved by each participating entity's Accountable Authority.

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

_____

Reviewed by Accountable Authority or in accordance with a resolution of the Governing Board of the Statutory Body

Principal Department (Sign and Date)

_____

Entity A (Sign and Date)

_____

Entity B (Sign and Date)

_____

Entity C (Sign and Date)

_____

Annexure I

Model Audit and Risk Committee Charter (Collaborative Shared Arrangement)

Audit and Risk Committees of NSW agencies are required to have a Charter that is consistent with the content of the 'model charter'. This model charter is based on the charter in Annexure B of this Policy and is for agencies entering into a collaborative shared arrangement. In doing so it is important that each agency consider carefully its particular circumstances, as there may be additional agency-specific requirements that shall also be addressed.

The following Accountable Authorities have entered into a shared arrangement and have established a shared Audit and Risk Committee ('the Committee') in compliance with the *Internal Audit and Risk Management Policy for the General Government Sector*.

Agency	Accountable Authority

For the purposes of this charter these organisations will herein be referred to collectively as "the participating entities".

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 Accountable Authorities of all participating entities by monitoring, reviewing and providing advice about the participating entities' governance processes, risk management and control frameworks, and external accountability obligations.

Authority

The Accountable Authorities of the participating entities authorise 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 Accountable Authorities of the participating entities at committee meetings
- obtain external legal or other professional advice, as considered necessary to meet its responsibilities, at the expense of any or all of the participating entities subject to the approval of the Accountable Authorities of the relevant participating entities.

Composition and tenure

The Committee will consist of at least three (3) members, and no more than five (5) members[61], who will be appointed by the process outlined in the Shared Arrangement Agreement.

The [Accountable Authority] of [participating entity as agreed in the Shared Arrangement Agreement] will appoint the Chair and members of the Committee. The Chair is counted as one member of the Committee.

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

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

Current employees of all NSW government sector agencies[62] other than State Owned Corporations cannot serve as members or chairs of an Audit and Risk Committee.

The members should collectively develop, possess and maintain a broad range of skills and experience relevant to the operations, governance and financial management of the participating entities, the environment in which the participating entities operate, and the contribution that the Committee makes to the participating entities.

At least one member of the Committee shall have accounting or related financial management experience with an understanding of accounting and auditing standards in a public sector environment.

Roles and responsibilities

The Committee has no executive powers.

The Committee is directly responsible and accountable to each particular Accountable Authority for the exercise of its responsibilities pertaining to that entity. In carrying out its responsibilities, the Committee shall at all times recognise that primary responsibility for the management of each participating entity rests with the Accountable Authority of that entity.

The responsibilities of the Committee may be revised or expanded in consultation with, or as requested by, the Accountable Authorities of participating entities from time to time.

The Committee's responsibilities in regards to each participating entity in the shared arrangement are to:

Risk management

- review whether management has in place a current and appropriate risk management framework that is consistent with *AS ISO 31000:2018*
- assess and advise on the maturity of the agency's risk management framework and risk culture
- consider the adequacy and effectiveness of the internal control and risk management frameworks by reviewing reports from management, internal audit and external audit, and by monitoring management responses and actions to correct any noted deficiencies
- review the impact of the agency's risk management on its control environment and insurance arrangements

61 Inclusive of the Chair.

62 Government sector is defined in the *Government Sector Employment Act 2013*.

- review the agency's fraud and corruption control framework including the fraud control plan and be satisfied that the agency has appropriate processes and systems in place to capture and effectively investigate fraud related information
- seek assurance from management that emerging risks (including, but not limited to, climate risk and cyber risk) are being identified and addressed
- seek assurance from management and Internal Audit that risk management processes are operating effectively, including that relevant internal control policies and procedures are in place and that these are periodically reviewed and updated
- review whether a sound and effective approach has been followed in developing risk management plans for major projects, programs or undertakings
- review whether a sound and effective approach has been followed in establishing the agency's business continuity planning arrangements, including whether disaster recovery plans have been tested periodically.
- review the significant risks arising from the strategic and operational activities of each agency that affect, or are likely to affect, other participating agencies in the shared arrangement and seek assurance that these risks have been communicated to relevant agencies in the shared arrangement and that these agencies have developed risk treatment measures.

External accountability

- assess the policies and procedures for management review and consideration of the financial position and performance of the agency including the frequency and nature of that review (including the approach taken to addressing variances and budget risks)
- review procedures around early close and year-end
- review the financial statements and provide advice to the [Accountable Authority] (including whether appropriate action has been taken in response to audit recommendations and adjustments) and recommend their signing by the [Accountable Authority]
- satisfy itself that the financial statements are supported by appropriate management signoff on the statements
- review the Chief Financial Officer Letter of Certification and supporting documentation (consistent with Treasury Policy Certifying the Effectiveness of Internal Controls Over Financial Information (TPP17-06))
- review cash management policies and procedures
- review policies and procedures for collection, management and disbursement of grants and tied funding.
- review the processes in place designed to ensure that financial information included in the [agency]'s annual report is consistent with the signed financial statements
- satisfy itself that the [agency] appropriately measures and reports on its performance against objectives and State Outcomes.[63]

Compliance and ethics

- determine whether management has appropriately considered legal and compliance risks as part of the [agency]'s risk assessment and management arrangements
- review the effectiveness of the system for monitoring the [agency]'s compliance with applicable laws, regulations and associated government policies
- seek assurance that the appropriate exercise of delegations is monitored and reviewed
- seek assurance that changes in key laws, regulations, internal policies and Accounting Standards affecting the agency's operations are being monitored at least once a year and appropriately addressed
- review the agency's process for communicating the code of conduct to staff and seek assurance as to compliance with the code
- review policies and processes for identifying, analysing and addressing complaints
- review whether management has taken steps to embed a culture which is committed to ethical and lawful behaviour.

[63] This includes consideration of Outcomes Budgeting measures such as Outcome Indicators and Program Performance Measures.

Internal audit

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

External audit

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

Responsibilities of members

Members of the Committee are expected to understand and observe the requirements of the Internal Audit and Risk Management Policy. Members are also expected to:

- make themselves available as required to attend and participate in meetings
- ensure they have the time and capacity to sufficiently cover all agencies in the shared Audit and Risk Committee including the time needed to study and understand the papers provided
- apply good analytical skills, objectivity and good judgement
- abide by the relevant ethical codes that apply to employment within the General Government Sector
- express opinions frankly, ask questions that go to the fundamental core of the issue and pursue independent lines of enquiry.

Reporting

The Committee will regularly, but at least once a year, report to each Accountable Authority participating in the shared arrangement or equivalent on its operation and activities during the year. Each report should include:

- an overall assessment of the agency's risk, control and compliance framework, including details of any significant emerging risks or legislative changes impacting the agency
- a summary of the work the Committee performed to fully discharge its responsibilities during the preceding year

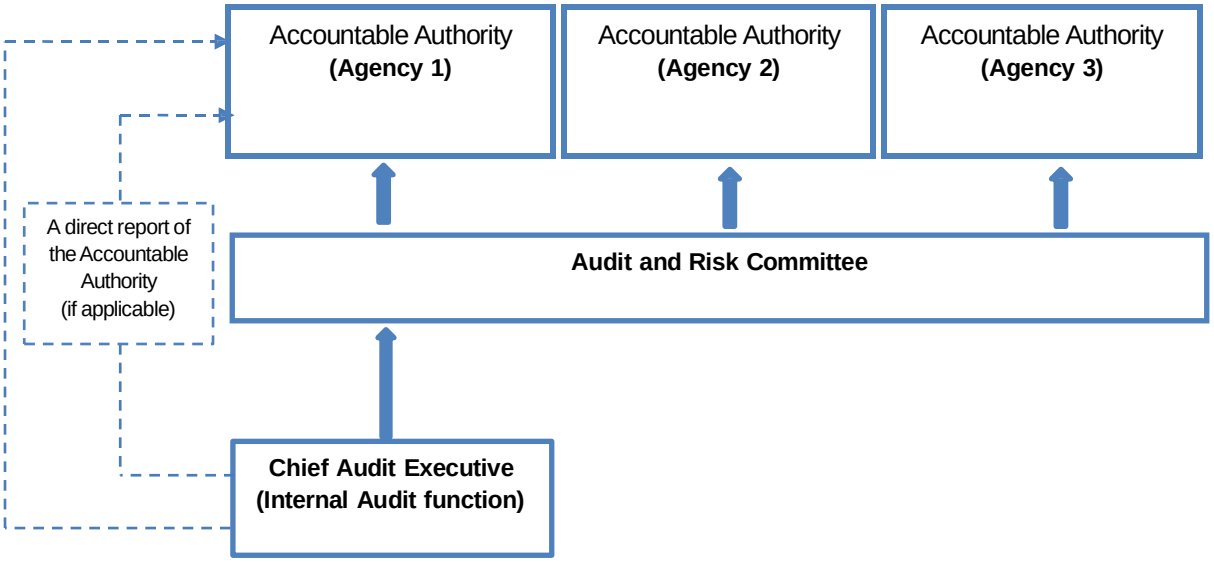
- details of meetings, including the number of meetings held during the relevant period, and the number of meetings each member attended
- a summary of the agency's progress in addressing the findings and recommendations made in internal and external reports
- a summary of the Committee's assessment of the performance of internal audit.

The Committee may, at any time, report to each participating entity's Accountable Authority on 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 any respective participating entity Accountable Authority.

Reporting Lines

The Committee shall 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 each participating entity's Accountable Authority on functional matters.

The following reporting line is prescribed where the dotted line represents the 'administrative' reporting line and the bold line represents the 'functional' reporting line:



Administrative arrangements

Meetings

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

The Chair is required to call a meeting if requested to do so by any participating entity's Accountable Authority, or another Committee member.

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

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

Attendance at meetings and quorums

A quorum will consist of a majority of Committee members.

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

The Accountable Authority of each participating entity may attend the meetings of the Audit and Risk Committee relevant to their agency. Committee members, if necessary, are able to have in-camera discussions. Each participating agency's Chief Audit Executive, Chief Risk Officer (as relevant), external audit representatives and any other agency representatives may attend Committee meetings relevant to their agency, except where the Committee members wish to have in-camera discussions. The Committee may also request the Chief Financial Officer and/or other representatives of participating entities to attend relevant committee meetings or participate for certain agenda items.

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

Dispute Resolution

Members of the Committee and each participating entity'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 Accountable Authorities of participating entities, the Chair may, as a last resort, refer the matter to Treasury to be dealt with independently.

Secretariat

Responsibility and the process for appointment of a person or persons to act as the Secretariat will be outlined in the Shared Arrangement Agreement. 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 shall 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 each participating entity's Accountable Authority stating they do not have any conflicts of interest that would preclude them from being members of the Committee.

Committee members shall 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 an actual, 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 participating entities' Accountable Authorities will agree upon 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 participating entities' Accountable Authorities) with appropriate input sought from the participating entities' Accountable Authorities, internal and external auditors, CROs (as relevant), management and any other relevant stakeholders, as determined by the participating entities' Accountable Authorities.

Arrangements for review of performance should be documented in the Shared Arrangement Agreement.

Review of charter

At least once a year the Committee will review this Charter. This review will include consultation with the Accountable Authorities of participating entities in the shared arrangement.

Any substantive changes to this Charter will be recommended by the Committee and formally approved by each participating entity's Accountable Authority.

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

_____

Reviewed by Accountable Authority or in accordance with a resolution of the Governing Board of the Statutory Body

Entity A (Sign and Date)

_____

Entity B (Sign and Date)

_____

Entity C (Sign and Date)

_____

Further information and contacts

For further Information or clarification on issues raised in the Policy, please contact:
Director, Financial Management Policy, Treasury
Telephone: 02 9228 5233
Email: finpol@treasury.nsw.gov.au