audit office
OF NEW SOUTH WALES

Internal Control Framework

October 2020

INSIGHTS FOR BETTER GOVERNMENT

contents

1.	Introduction	2
2.	What is an internal control framework?	2
3.	Why have an effective internal control framework?	2
4.	Three lines model	3
5.	Responsibilities	4
6.	Components of internal control	5
7.	Limitations of internal control	8
8.	Annual CFO certification and management control questionnaire	9
9.	Contact Point	9
10.	Review	9

1. Introduction

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) released its most recent version of the Internal Control – Integrated Framework in 2013. It is still recognised as a leading framework for designing, implementing, and conducting internal control and assessing the effectiveness of internal control.

The Audit Office's Internal Control Framework is based on the internal control guidelines recommended by the COSO as adopted by the auditing profession as their definition of internal control.

2. What is an internal control framework?

COSO defines internal control as 'a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.'

This definition reflects certain fundamental concepts. Internal control is:

- geared to the achievement of objectives
- a process consisting of ongoing tasks and activities - a means to an end, not an end in itself
- effected by people - not merely about policy and procedures, systems, and forms, but about people and the actions they take at every level of the Audit Office to affect internal control
- able to provide reasonable assurance - but not absolute assurance, to an entity's senior management and the Office Executive
- adaptable to the entity structure - flexible in application for the entire Audit Office, branch, unit or business process.

An effective internal control system provides reasonable, but not absolute, assurance that assets are safeguarded, financial and other information is reliable, laws, directions and Audit Office policies are being complied with and that errors and fraud are prevented.

3. Why have an effective internal control framework?

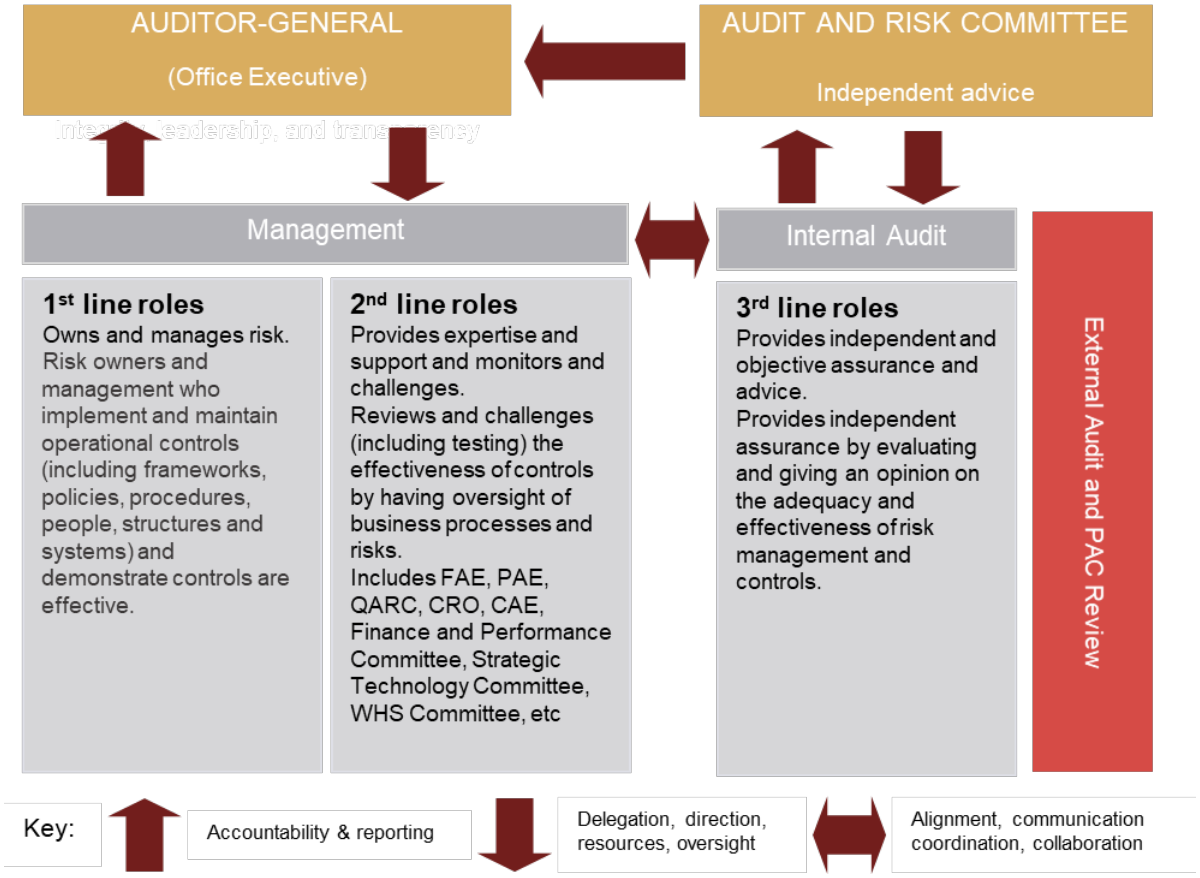
Internal controls are used to help the Audit Office achieve its corporate objectives. By identifying risks that will prevent these corporate objectives being achieved, we can identify what effective controls we need to have in place.

Effective internal controls help to mitigate, but not limited to the following risks:

- **Reputational risk** – so that the Audit Office continues to be recognised for its independence and integrity and the value it delivers through high quality independent assurance services.
- **Strategic and Operational risks** – so that the Audit Office's corporate objectives are achieved, resources are acquired economically and employed efficiently, and quality business processes and continuous improvement are emphasised.
- **Fraud risk** – so that the Audit Office's resources, including its people, systems and information, are adequately protected.
- **Compliance risk** – so that the actions of all staff comply with Audit Office policies, procedures and all relevant laws, standards, central agency directions and applicable Auditor-General's report recommendations.
- **The risk of error in the Audit Office's financial statements** – so that internally and externally published information is accurate, reliable and timely.
- **Cyber security risks** – so that confidential and sensitive information is secure.
- **Work, health and safety risks** – so that the physical and mental health of staff is protected.

4. Three lines model

The Three Lines Model issued by the Institute of Internal Auditors, provides a simple and effective way to communicate the roles and responsibilities surrounding risk and controls within the Audit Office to achieve our objectives. The Three Lines Model helps to identify structures and processes that best assist the achievement of objectives and facilitate strong governance and risk management.



The elements in the three lines model are:

1. **First line of defence: owns and manages**

   Comprises of senior management and risk owners who implement and maintain operational controls in each branch or unit or specific areas of responsibility. This involves Directors and Executive Managers but may also include risk owners within specific functions such as WHS or Information Security.

2. **Second line of defence: oversees**

   Comprises specialist functions that are independent of the first line of defence and challenge and provide oversight over business processes and risks. This will include the Chief Risk Officer, Chief Finance Officer, Quality Audit Review Committee, and Project Steering Committees.

3. **Third line of defence: provides independent assurance**

   Comprises independent assurance that the first and second lines of defence are operating effectively, and improvements are identified and recommended. This includes the internal audit function and peer reviews which provide independent assurance on the appropriateness and effectiveness of the risk management and control framework.

The Auditor-General through the Office Executive and Chief Risk Officer provides the governance structure, sets the risk appetite and establishes the risk management culture.

The Audit and Risk Committee role is to provide independent assistance to the Auditor-General by monitoring, reviewing and providing advice about the Audit Office's governance processes, risk management and control frameworks. It does this by oversight and review of the results from the three lines of defence, and more specifically through direct reports from Internal and External Audit.

5. Responsibilities

The **Auditor-General** has ultimate responsibility for ensuring an effective system of internal control over the financial and related operations of the Audit Office, in line with the requirements of the *Government Sector Audit Act 1983* (GSA Act).

The **Deputy Auditor-General** has responsibility for the Audit Office's Internal Control Framework.

The **Office Executive** is accountable for oversight of internal control by establishing policies and expectations of conduct, setting the tone at the top and managing the Audit Office's strategic risks. The Office Executive is responsible for ensuring necessary controls and treatment plans are in place to effectively manage risk. Members of the Office Executive also attend Audit and Risk Committee meetings as requested to discuss the current management of specific risks and internal controls.

The **Chief Finance Officer (CFO)** is responsible for conducting the annual management internal control questionnaire as part of the annual CFO certification as to the effectiveness of the system of internal control over financial information.

The **Executive Manager, Governance (Risk and Internal Audit)**, on behalf of the **Chief Risk Officer and Chief Audit Executive**, prepares status reports for the Office Executive and Audit and Risk Committee as required regarding the Audit Office's Internal Control Framework, Risk Management Framework and Internal Audit Function.

The **Audit Office Leadership Team** (including Directors, Executive Managers, CFO and CIO) are responsible for contributing and achieving the Audit Office Strategic Plan; and establishing, documenting, assessing and maintaining internal controls that mitigate risk within their team and ensuring staff in their team, have complied with applicable Audit Office policies. The Audit Office Leadership Team part of the first line of defence.

Audit Office Leadership team members may have either a primary or secondary responsibility in ensuring compliance with Audit Office policies. Primary responsibilities exist where a policy relates directly to a person's role or area of expertise. While secondary responsibility exists where Audit Office Leadership team members have responsibility for specific aspects of policy implementation by ensuring team members adhere to or conduct activities in accordance with relevant policies.

For example, the Audit Office Leave Policy is owned and managed by the Executive Manager HR, who is responsible for Audit Office wide implementation and awareness of the policy, and providing advice and training where needed. While a Director or Executive Manager is responsible for reviewing and approving leave entitlements in accordance with the leave policy.

All **Audit Office staff** including temporary staff and contractors must comply with internal controls and applicable Audit Office policies within the scope of their roles. They are also responsible for reporting to management instances where they consider internal control procedures are not adequate or are not being complied with.

The Audit and Risk Committee is responsible provide independent assistance to the Auditor-General by monitoring, reviewing and providing advice about the Audit Office's governance processes, risk management and control frameworks.

6. Components of internal control

The Audit Office has five primary components of internal controls based on the COSO guidelines:

- Control Environment
- Risk Assessment
- Control Activities
- Information and Communication
- Monitoring.

6.1 Control Environment

A control environment, where competent people understand their responsibilities and authority and are committed to acting appropriately, will provide a foundation for internal controls to exist and operate effectively. The Office Executive establishes the tone at the top regarding the importance of internal control including expected standards of conduct. Management reinforces expectations at the various levels of the organisation. To ensure all Audit Office staff are aware of their responsibilities, training and updates are provided on a timely basis and applicable Audit Office policies and procedures are published on the Audit Office intranet. An effective internal control environment for the Audit Office includes:

- the Office Executive provides governance oversight by having appropriate management philosophy and operating style, providing the right tone at the top regarding the importance of internal controls and ensuring the development and performance of internal controls
- maintaining integrity and ethical values (refer to the Code of Conduct, Corporate Values and related policies such as the Conflict of Interest Policy and other employee conduct and obligations policies)
- processes to attract, develop and retain competent people through appropriate selection processes, regular performance reviews, learning development programs and adequate training
- establishing structures, reporting lines and appropriate authorities and responsibilities to meet objectives (including the Delegations Manual)
- complying with relevant laws, central agency directions (see Compliance Policy and Register), applicable Auditor-General report recommendations, and Audit Office policies, instructions and guidance as found on the intranet
- strategic and business planning processes to hold individuals accountable for their internal control responsibilities in order to meet the Audit Office's objectives by having rigour around performance measures and incentives (refer to Audit Office Corporate Plan).

6.2 Risk Assessment

The Audit Office applies an enterprise wide risk management framework where risk management is embedded within the Audit Office's overall strategic and operational policies and practices. A key component of the risk management framework is the strategic and operational risk reports which captures the results of risk assessments made at both these levels. It does this by:

- establishing the context
- identifying risks
- analysing risks
- evaluating controls
- determining mitigating actions, if any, to be taken to address gaps in Audit Office processes.

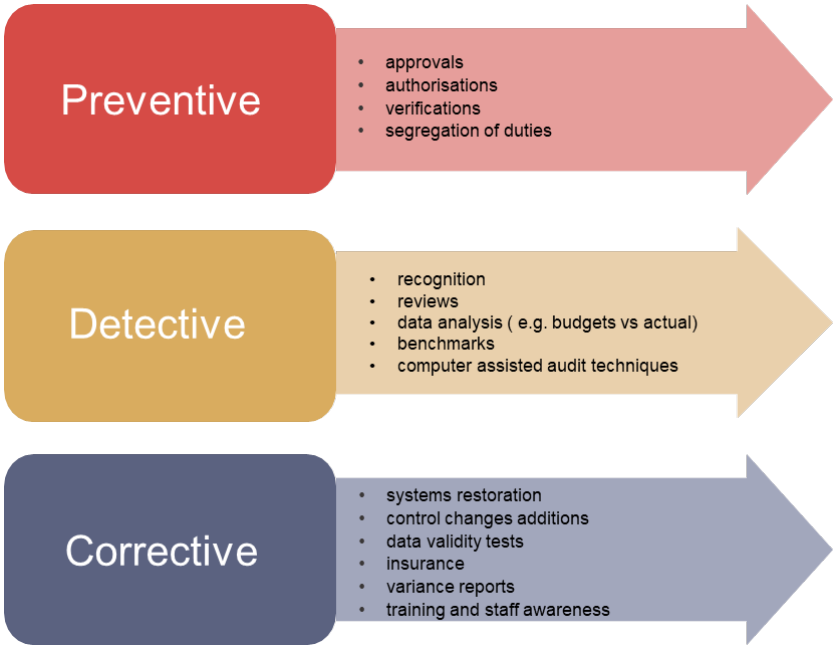
The responsibility and accountability for each risk is allocated to a risk owner who must have oversight and ensure mitigating controls are appropriately designed, operating effectively and corrective action is taken where gaps are identified.

The Audit Office's specific risk policies and reports can be found on the Audit Office's intranet and include:

- Risk Management Framework
- Strategic and operational risk reports and registers
- Risk Appetite Statement
- Fraud Control Risk Assessment
- Compliance Register.

6.3 Control Activities

Control activities are incorporated in the Audit Office's policies, procedures and practices. Controls can be classified as those before the event as preventive, or after the event as detective or corrective. Examples of each of these are:



Control activities are also incorporated specifically in audit assurance policies, procedures and guidelines and include:

- using risk-based methodologies that comply with Australian Auditing Standards and other professional and legislative requirements
- having ethical and independence policies and procedures
- requiring staff to meet professional qualification requirements
- a specialist audit support function
- structured staff training
- merit based progression through a performance management system
- peer, hot and cold reviews (see 6.5.6 below).

6.4 Information and Communication

The Audit Office's intranet and website, Office Forum, professional development programs, strategic and business processes, information systems and the Leadership Team, identify, capture and communicate information that enables people to meet the requirements of their job.

6.5 Monitoring

The Audit Office has a number of oversight bodies and quality assurance processes including:

- Office Executive
- Audit and Risk Committee
- internal audit
- external audit
- PAC Quadrennial Reviews
- ACAG peer reviews
- Quality Assurance Framework and Quality Audit Review Committee (QARC)
- other Audit Office Committees (such as WHS Committee, Remuneration Committee, Finance and Performance Committee, Strategic Technology Committee, L&D Committee, etc).

6.5.1 Office Executive

The Office Executive assists the Auditor-General to meet their statutory responsibilities and provides leadership to the Audit Office in pursuing its strategic direction and delivering against the Corporate Plan. The Office Executive's primary objectives and corporate governance functions include:

- setting and monitoring progress against the Office's vision, purpose, values and strategic objectives
- setting direction on key changes to the Audit Office's operating environment that are expected to have a whole-of-office impact
- ensuring the Office is compliant with relevant law, directions, codes and practices
- operating in accordance with the Audit Office's values.

For more information on the role of the Office Executive refer to the Office Executive Charter.

6.5.2 Audit and Risk Committee

The Audit and Risk Committee is an independent committee of the Audit Office and reports directly to the Auditor-General. The objective of the Audit and Risk Committee is to provide independent assistance to the Auditor-General by monitoring, reviewing and providing advice about the Audit Office's:

- governance processes
- risk management and control frameworks
- its external accountability obligations including financial reporting
- compliance with applicable laws and regulations
- internal and external audit.

For more information on the role of the Audit and Risk Committee refer to the Audit and Risk Committee Charter.

6.5.3 Internal Audit

Internal audit provides independent and objective assurance to management on the adequacy of internal control, risk management, financial reporting systems and governance processes through:

- reviewing and reporting on the adequacy and effectiveness of the Audit Office's system of internal control to manage risk
- recommending improvements to any identified control weaknesses and improve business performance.

For more information on the role of the internal Audit Function refer to the Internal Audit Charter.

6.5.4 External Audit

External audit provides an independent audit of the Audit Office's financial statements in accordance with Australian Auditing Standards and includes:

- obtaining audit evidence about the amounts and disclosures in the Audit Office's financial statements
- assessing the risk of material misstatement of the Audit Office's financial statements
- considering the internal controls relevant to the preparation and fair presentation of the Audit Office's financial statements
- evaluating the appropriateness of the accounting policies used to prepare the Audit Office's financial statements
- evaluating the reasonableness of accounting estimates made in the preparation of the Audit Office's financial statements
- issuing an opinion on the Audit Office's financial statements in accordance with relevant accounting standards and other requirements.

6.5.5 PAC Quadrennial Review

A quadrennial review of the Audit Office is conducted by a person appointed by the Public Accounts Committee under section 48A of the GSA Act. The review is to examine the auditing practices and standards of the Auditor-General and to determine whether the Auditor-General is complying with those practices and standards in the carrying out of the Auditor-General's functions under the Act.

6.5.6 ACAG peer reviews

The Audit Office participates in a peer review program with other Australian audit offices who regularly review our performance and financial auditing processes under the quality assurance framework, sponsored by the Australasian Council of Auditors General (ACAG). The Audit Office implements recommendations from the reviews to address identified gaps.

6.5.7 Quality Assurance Framework and Quality Audit Review Committee (QARC)

The system of quality control is an important mechanism to ensure the Audit Office and its staff comply with Australian Auditing Standards, relevant ethical requirements, and applicable legal and regulatory requirements; and to ensure our reports are appropriate in the circumstances. QARC is a key component of the Audit Office's Quality Assurance Framework.

For more information on the Quality Assurance Framework refer to Audit Office policy and for information on the role of the QARC refer to the QARC Charter.

6.5.8 Other Audit Office Committees

The Audit Office has a number of other committees with responsibilities for providing expertise and support and monitors and challenges through oversight of specific functions or areas. These committees include:

- Work Health and Safety Committee
- Remuneration Committee.
- Finance and Performance Committee
- Strategic Technology Committee
- Learning and Development Committee

7. Limitations of internal control

Internal control is designed and implemented to provide reasonable assurance that the objectives and goals of the Audit Office are achieved. It is acknowledged that there are inherent limitations of internal control which include:

- resource constraints

- human judgement and errors
- manual and automated controls that can be circumvented by collusion
- inappropriate overriding of internal controls by staff or management.

8. Annual CFO certification and management control questionnaire

As part of the preparation of the annual financial statements, the CFO provides the Auditor-General with an annual Letter of Certification as to the effectiveness of the system of internal control over financial information. The CFO Letter of Certification is supported by a management internal control questionnaire, which is completed by the members of the leadership team.

9. Contact Point

If staff have any questions about this framework, they should contact the Executive Manager, Governance (Internal Audit and Risk).

10. Review

It is intended that this policy will be reviewed every two years or earlier if significant new information, legislative or organisational change warrants an update to this framework.