audit office
OF NEW SOUTH WALES

Risk Management Framework

Version: 2.0

Date: 18 June 2024

Review date: June 2026

contents

1. Policy and commitment statement

The Audit Office of NSW (the Audit Office) is committed to managing its strategic, operational and project risks. This allows us to make informed decisions, minimise threats and embrace opportunities that are presented, adapt to change, and ultimately achieve our corporate objectives.

The Audit Office recognises that risks (and opportunities) are inherent in everything we do. As an independent integrity agency, we aim to responsibly take the right level of risk in accordance with our risk appetite.

This Risk Management Framework (RMF) is endorsed by the Auditor-General with the full support of the Office Executive, who together are committed to embedding risk management principles and practices across the Audit Office.

All employees are responsible for positively engaging with risk and actively identifying, reporting and escalating risks and opportunities within their area/s of responsibility.

2. Objective

The objective of this RMF is to ensure that we adequately manage risk across all parts of our business in a structured and consistent way and in accordance with Australian standard AS ISO 31000:2018 *Risk Management – Guidelines* (ISO 31000). It aims to:

- support informed decisions
- underpin effective and efficient operations
- safeguard our people, assets, and other resources
- maintain our reputation and the trust the NSW parliament and citizens have in us
- prevent operational disruptions and maintain business continuity.

2.1 What is risk?

ISO 31000 defines risk as 'the effect of uncertainty on objectives'. The effects can be positive, negative or both, and hence create both risks and opportunities.

The Audit Office's strategic objectives are outlined in the Audit Office's Corporate Plan. The Audit Office's strategic risks are those uncertainties that could prevent or assist the Audit Office in achieving its Corporate Plan, including its vision, purpose, and future state.

2.2 What is risk management?

Risk management is the identification, analysis, assessment and evaluation of risks and opportunities and is built into everything we do, especially in informing our decisions. The objective is to reduce the impact of risks while realising opportunities to ensuring our overall objectives are met. At the Audit Office risks are seen as an enabler and not a hindrance.

3. Scope

This RMF applies to all business operations and activities of the Audit Office and to all Audit Office employees (that is persons employed under the Award conditions or on executive contract), and contingent workers, within the context of their area/s of responsibility.

4. Risk management guiding principles

In specifying the Audit Office's approach to risk management, the RMF outlines the following principles, tailored from the principles in ISO 31000:

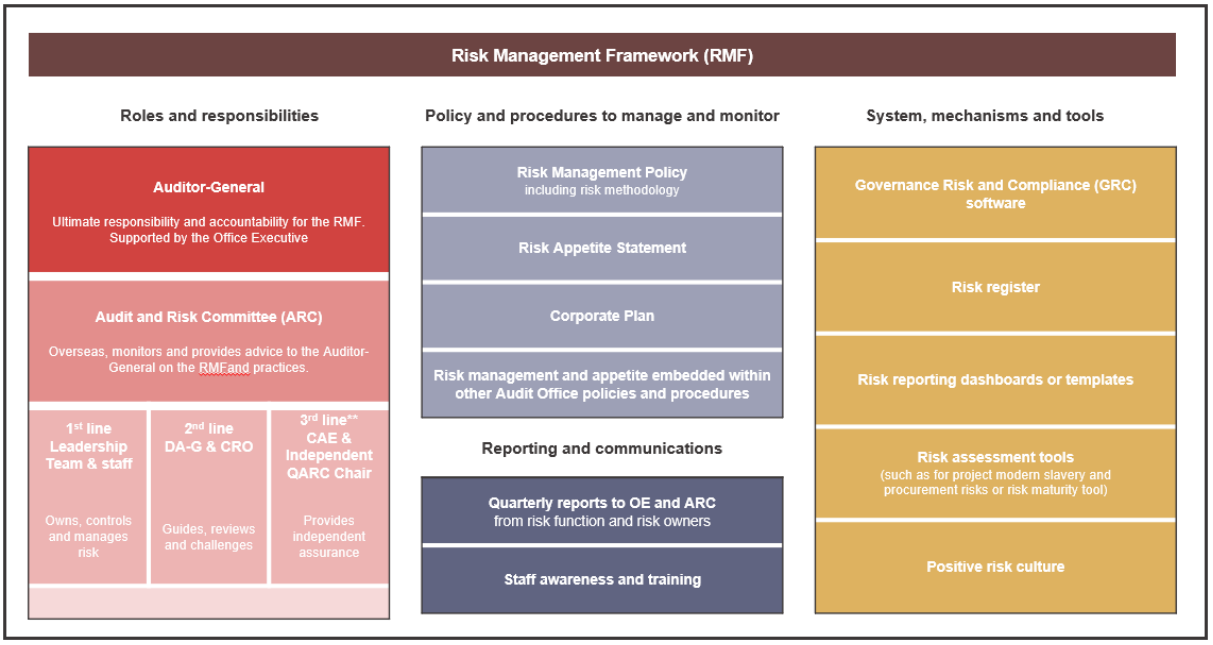
1. **Integral to the governance framework** – risk management is a key part of the Audit Office's governance framework, and the RMF assigns clear accountabilities and responsibilities.
2. **Enterprise wide** – risk management is integrated in everything we do and in everyday decisions, including but not limited to activities involving strategic planning, budgeting and financial management, project management, quality assurance, audit and assurance

engagements, work health and safety, fraud and corruption control, information security, procurement, etc.

3. **Consistent and effectively applied** – risk methodologies and tools outlined in the RMF are consistently and appropriately applied at all levels.
4. **Positively embedded in our culture** – a risk-aware culture is instilled where risk management is seen as a positive attribute of decision-making and is an enabler rather than a corrective or stop measure.
5. **Dynamic** – risk management is an iterative process that responds swiftly to changing internal and external environmental factors and events, new knowledge or understanding, results of monitoring and reviewing activities, new and emerging risks and opportunities and other factors that change or disappear.
6. **Supported by best available information** – risk management draws on diverse sources of information (historical and current), sound judgement, analytics and input from all relevant stakeholders, but recognises limitations of data.
7. **Compliant with the regulatory framework** – the RMF is aligned to ISO 31000 as required by *TPP 20-08 Internal Audit and Risk Management Policy for the General Government Sector* (TPP 20-08) and best practice guidelines.
8. **Tailored** – the RMF is fit for purpose and commensurate to the Audit Office's risk profile, size, complexity, and operating environment.
9. **Continually improved** – risk management leads to the continual improvement of operations through the revision of processes, actions and controls as well as continual improvement to the maturity of risk management.

5. Components of the RMF

The RMF is made up of roles and responsibilities, policies and procedures, systems and tools and, reporting and communication activities, that together ensure risks (and opportunities) are identified, assessed and managed to acceptable levels. The diagram below outlines the components of the RMF.



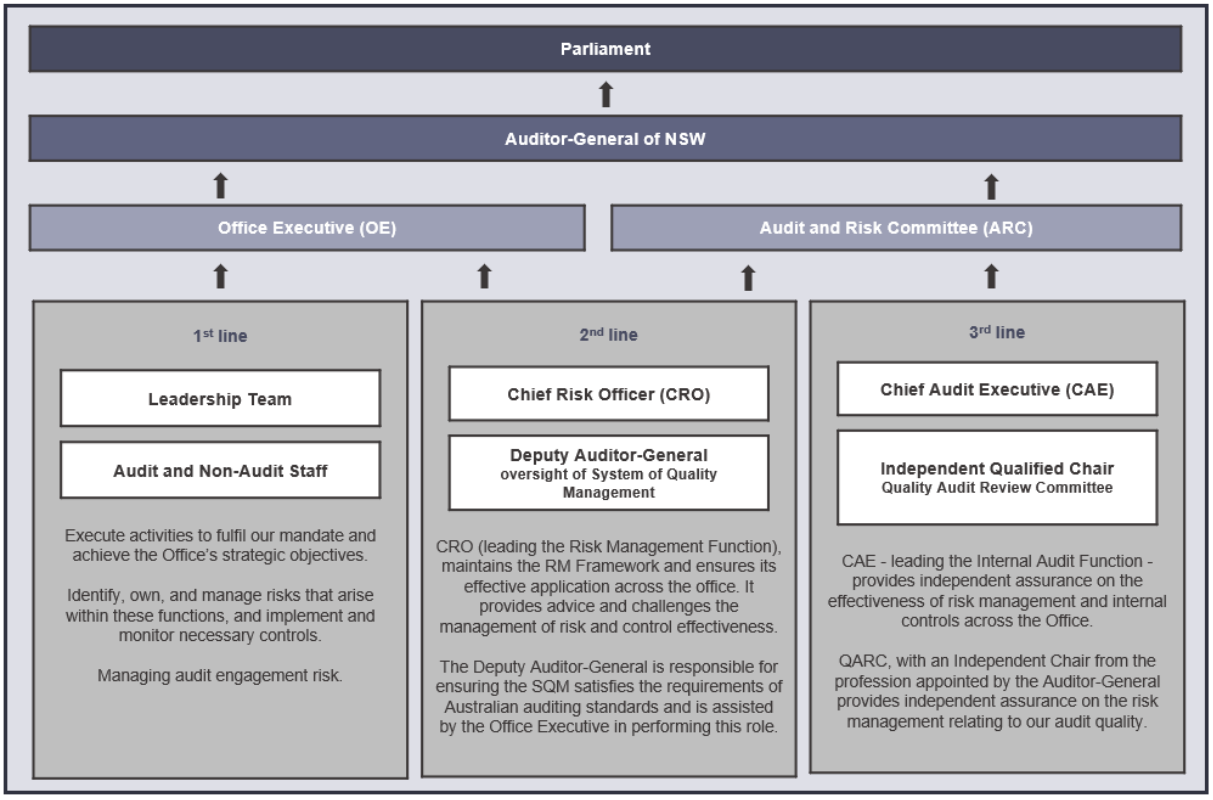
6. Roles and responsibilities

Based on the first risk management guiding principle outlined in section 4, that risk management is *integral to the governance framework,* the RMF assigns clear accountabilities and responsibilities and provides guidance on risk escalation and management. It does this using the Three Lines Model.

6.1 Three lines model

The Audit Office has adopted the Three Lines Model to assign roles and responsibilities for risk management. Refer to section 10.4 for the Three Lines Model used to assign roles and responsibilities for controls.

Everyone is required to apply the RMF within the context of their area/s of responsibility.



6.2 Roles and responsibilities

6.2.1 Auditor-General

The Auditor-General is ultimately responsible and accountable for the RMF and ensures 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).

With the support of and consultation with the Office Executive and Chief Risk Officer, the Auditor-General:

- leads and promotes a positive risk culture
- approves the RMF
- authorises the Audit Office's risk appetite
- has oversight and manages strategic risks.

6.2.2 Office Executive

The Office Executive support the Auditor-General in the effective management of risk and the promotion of a positive risk culture. More specifically they are responsible for:

- overseeing how risks faced by the Audit Office are being managed and ensuring the Audit Office operates within the risk appetite
- having oversight of strategic risks as a strategic risk owner and overseeing operational risks within their area of responsibility, branch or as sponsors for projects or initiatives. This will include identifying, assessing and managing risks, with support from the Risk Management Function within Governance, and ensuring a reasonable level of assurance that controls are effective in design and operation

- providing resources necessary to ensure the day-to-day identification, assessment, and management of risks
- oversight of internal controls by establishing policies, procedures, and expectations of conduct and setting the tone at the top.

6.2.3 Audit and Risk Committee

The Audit and Risk Committee (ARC) provide independent assistance to the Auditor-General by reviewing, seeking assurance, and providing advice about the RMF, practices and internal controls. It is guided by TPP 20-08 and its Charter.

6.2.4 First line – Risk owners including the Leadership Team

The risk owner is the person assigned as the lead for the management and/or oversight of a risk, including completing and reporting on a formal risk assessment for their respective risk/s. Risk owners can relate to strategic risks (who will be a member of the Office Executive), operational risks (who can be anyone assigned to a risk relating to either a branch, business area or function) or project risks.

Risk owners are responsible for the overall coordination of the management of the risk/s including:

- obtaining assurance that controls are effective (in design and operation) to manage the risk to an acceptable level
- obtaining assurance that mitigation plans are progressing into established controls
- monitoring the environment to identify emerging pressures, opportunities as they arise or changes to risks (positive or negative)
- reporting and presenting at the Office Executive and ARC meetings as required under the annual risk reporting schedule.

6.2.5 First line – audit and non-audit staff

All employees, including audit staff, are responsible for positively engaging with risk and actively identifying, reporting and escalating risks within their area/s of responsibility. This means:

- being alert to existing or emerging risks when conducting activities or making day-to-day decisions within their area
- implementing controls and complying with Audit Office policies and procedures to reduce those risks
- understanding and applying the RMF and attending relevant training
- operating within the Audit Office's risk appetite statement when making decisions and carrying out duties and responsibilities
- escalating changes to existing risks, identified emerging risks, incidents, breaches or other developments that could create a risk and instances where internal control procedures are not adequate or are not being complied with.

6.2.6 Second line - Risk Management Function

The Risk Management Function provides risk management support to the business, so that risk owners can manage and report on their risks in line with the RMF.

The members of the Risk Management Function are subject matter experts on risk management providing advice and guidance rather than conducting risk management on behalf of the business and include the Chief Risk Officer and Governance Manager.

6.2.6.1 Chief Risk Officer (CRO)

The Chief Risk Officer (Director, Governance and Risk) is responsible for leading the Risk Management Function and reports to the Deputy Auditor-General for the purposes of the RMF.

CRO responsibilities include:

- developing, implementation, and reviewing the RMF in line with relevant government policies, standards, and better practice. This occurs in consultation with the Office Executive, and other key stakeholders in addition to any advice from the ARC

- supporting and providing advice in applying the RMF
- overseeing the continuous improvement of risk management capability and awareness across the Audit Office
- challenging and offering alternative views in any activities or decisions that may impact the Audit Office's exposure to risk and opportunities.

6.2.6.2 Governance Manager

Governance Manager assists the CRO in administering the day-to-day activities of the Risk Management Function. This includes:

- assisting the CRO in the update and application of the RMF
- maintaining the annual risk reporting schedule and co-ordinating strategic, operational and project risk management reports from the risk owners for submission to the Office Executive and ARC
- maintaining the risk register
- assisting in the development and roll out of relevant staff training.

6.2.7 Second line – Deputy Auditor-General oversight of System of Quality Management (SQM)

The Deputy Auditor-General is responsible for ensuring the SQM satisfies the requirements of Australian auditing standards and is assisted by the Office Executive in performing this role.

Policy and guidance is provided in the Audit Office's Audit and Assurance policies, risk based audit methodology and System of Quality Management.

6.2.8 Third line – Chief Audit Executive oversight of Internal Audit Function

The Internal Audit Function is led by the Chief Audit Executive and provides independent and objective assurance to the Auditor-General and ARC on the effectiveness of the RMF, including the design and operational effectiveness of internal controls. It does this through its annual internal audit program by:

- evaluating the effectiveness of, and contributing to the improvement of, risk management and internal control processes
- identifying findings and risk exposures and making recommendations to remedy mitigating controls.

Refer to the Internal Audit Charter for further details.

6.2.9 Third line – Independent Qualified Chair of the QARC

The Quality Audit Review Committee (QARC) has an independent chair from the profession appointed by the Auditor-General and is established to:

- monitor the quality of audit and assurance products and provide reasonable assurance of compliance to the requirements of ASQM 1 'Quality Management for Firms that Perform Audits or Reviews of Financial Reports and Other Financial Information, or Other Assurance or Related Services Engagements' and, if applicable, ASA 220 'Quality Management for an Audit of a Financial Report and Other Historical Financial Information.'
- review the effectiveness and efficiency of the quality review process.

For specific roles and responsibilities of QARC, refer to the QARC Charter.

7. Risk appetite statement

Risk appetite is the amount of risk an organisation is prepared to accept to achieve its strategic objectives and business plans. It articulates and makes clear the boundaries which the Audit Office is willing to operate in and guides decision making.

A clear and understood risk appetite empowers individuals and the business to carry out its activities and make sound decisions – freedom with boundaries.

The Auditor-General is responsible for authorising the Audit Office's risk appetite, which is outlined in the Risk Appetite Statement (RAS).

7.1 Risk appetite levels

Staff must apply the RAS to inform decisions in the pursuit of achieving strategic and operational objectives. The risk appetite will be different for different risk areas and will be dependent on several factors such as the importance of the objectives, the consequence of a risk event occurring, or the cost-benefit trade off.

When reporting internally on the status of risks, the risk appetite is often referred to as the 'acceptable risk' and compared with the 'residual risk'.

For the Audit Office, the different risk appetite levels can be defined as follows:

Risk appetite	Definition
High	Willingness to be exposed to a heightened level of risk and uncertainty for potentially greater rewards or when pursuing opportunities or innovating. This is generally not an appetite adopted by the Audit Office.
Medium	Willingness to be exposed to some level of risk for an acceptable level of reward. The Audit Office will take on some risk to operate in this area or in this way after options are considered and the most appropriate option selected for an acceptable level of reward. This is adopted for some corporate and management activities.
Low	Uncertainty and risks are minimised. The Audit Office may operate in this area or in this way where the value is assessed as worthwhile, and only after risks or uncertainty have been mitigated or minimised as low as is practicable. This is adopted for core business activities within financial and performance audit and some corporate and management activities.
No appetite	No willingness to take on any risk. The Audit Office will not operate in this area or in this way. This is adopted for activities that constitute fraud and corruption or actions which deliberately and substantially jeopardise our independence and reputation as an integrity agency.

The level of risk the Audit Office is willing to accept should also be outlined in Audit Office policies to guide ways of operating, decision-making and business approaches. Policies should be aligned with the Audit Office's overarching RAS and be clear on the risk appetite and the desired risk culture for the specific area covered by the policy.

7.2 Risk tolerances – operation of the RAS

Risk tolerances are the boundaries for risk taking expressed as a specific measurable threshold. Risk tolerances define how the RAS is to be applied in everyday business activities, when making decisions or executing responsibilities or functions.

Staff are expected to operate within the set risk tolerances.

It is recognised that situations may occur that result in operating **outside** or **approaching** the boundaries of the risk appetite. Each situation must be assessed, and an appropriate response taken that is guided by the following:

Tolerance	Response
Operating **within** risk appetite	Accept and no further action or escalation needed. Continue to monitor the risk as normal.

Tolerance	Response
Approaching the boundaries of the risk appetite	Escalate to your manager and the Office Executive on a timely basis with any continued reporting as required. Increase monitoring and review controls. Identify actions to avoid operating outside the risk appetite. Share information with relevant staff to raise awareness.
Outside the risk appetite	Escalate to your manager and the Office Executive immediately and continue to regularly report until operating back within the risk appetite. Treat by implementing corrective actions which may include adopting additional controls. Share information with relevant staff to ensure lessons learnt where applicable.

8. Risk culture

Organisational culture refers to a set of shared values, behaviours, norms, beliefs, and practices that characterise the functioning of a particular organisation. Risk culture refers to the set of shared values and behaviours that characterise how an organisation considers risk in its day-to-day activities. However, the risk culture should be embedded into and not separate from the organisational culture.

The Audit Office adopts a positive risk culture, where risk management is seen as a positive attribute of decision-making and an enabler rather than a corrective or stop measure. Staff must be encouraged and supported to engage effectively and positively with risk.

The Audit Office's risk culture also reflects its core values, in particular *Courage (even when its uncomfortable)* and *Curious and Open Minded*.

8.1 A risk-aware culture and training

All staff must be familiar with the RMF and adopt its approach. This includes continuously scanning the environment for changes to existing risks or emerging or new risks and escalating these to management, along with any incidents, breaches or other developments.

Staff are required to complete mandatory risk training as directed. This may include direct risk management training or training for a specific area of risk like cyber awareness. This ensures staff awareness and risk management capabilities are maintained. In addition, one-on-one training and advice is provided by the CRO in applying the RMF to everyday activities.

The Audit Office adopts a risk-based audit methodology. Risk training for auditors when conducting audit and assurance engagements, is embedded throughout the learning and development program for audit staff. This includes any mandatory audit methodology training, meeting professional education requirements, and audit and assurance policies and guidance available to all audit staff.

8.2 Attributes of a positive risk culture

While the Auditor-General is ultimately responsible for setting the desired risk culture, all staff have a role to play. Attributes and actions that are encouraged to support a positive risk culture at the Audit Office include:

Cultural attributes	Management actions	Staff actions
Instil shared values and purpose	Provide a **positive tone at the top** - commitment and model sound risk management practices and business decisions. See risk events as an **opportunity to learn** and **embrace innovation or opportunities** within the risk appetite.	**Positively engage with risk and opportunities** and feel empowered and confident to manage risks within areas of responsibility. **Be alert** to potential risks or opportunities.
Foster open communication	Have an **open-door policy and open mind** supporting a safe environment	**Confidently escalate** risks, breaches, or opportunities.

Cultural attributes	Management actions	Staff actions
	where staff can openly discuss risks or breaches. **Reward staff** that actively seek to understand and manage risks and opportunities. Provide **constructive feedback.** **Promptly respond to complaints.**	
Adopt a consistent and embedded approach	**Endorse and advocate** the RMF. Provide **adequate resources** with clear risk responsibilities through job descriptions and performance agreements. **Risk is integrated** in everything we do including making informed decisions and strategy and risks are strongly aligned. **Monitor and review risks and mitigating controls.** **Ensure business systems and processes are fit for purpose** and commensurate with the risk.	**Understand** the RMF. **Know your risk responsibilities.** **Understand** the risks and mitigating controls within your area of responsibility.
Promote risk awareness	Provide **adequate training** for all staff to develop risk capabilities. **Share risk information and knowledge**, learnings, and best practice.	**Attend risk training** as required. **Learn** from incidents or risk events.

9. Risk management process

The Audit Office risk management process adopts the methodology in ISO 31000. It provides a systematic approach to identifying, analysing and evaluating risks (and opportunities) so that they can be appropriately treated or exploited.

Risk and opportunity assessments should be conducted at different levels across different areas and activities, including but not limited to:

- developing corporate and branch business plans
- developing the audit work program and in conducting financial and performance audits
- managing work health and safety
- investigating any breaches or incidents
- conducting procurement activities including assessing for modern slavery
- undertaking business continuity and disaster recovery planning
- budgeting and financial management
- assessing information and system security
- preventing fraud and corruption
- developing or revising policies, procedures and guidelines
- making key business decisions
- managing projects.

An overview of the Audit Office's risk management process is detailed below.

9.1 Step 1: Scope, context, criteria

Define the objective the risk assessment is trying to achieve. This will usually involve:

- considering the strategic objectives in the Corporate Plan or operational or activity objectives.

  For example, an objective could be to keep our staff safe. Hence this provides the context and scope when assessing work, health, and safety risks.
- consulting with key stakeholders
- conducting an environmental scan to understand the context in which we operate.

9.2 Step 2: Risk assessment

Step 2.1: Risk identification

Risks and opportunities are to be identified by examining potential sources, causes and impacts. This can be done in several ways such as through an environmental scan, consulting key stakeholders, examining complaints, conducting surveys, reviewing the results from inspections and investigations, root cause analysis of incidents or breaches, internal and external audits or other independent reviews, etc.

The aim is to identify possible risks and opportunities.

Step 2.2: Risk analysis

A risk analysis involves understanding in more detail the identified risks and opportunities from step 2.1 and determining the level of risk using the risk matrix in Appendix 3.

The risk analysis includes an understanding of:

- what can happen – the risk event or opportunity
- how can it happen – identifying the causes and sources of the risk event or opportunities
- what is the affect if it were to happen – consequence (or impact)
- how often will it happen – likelihood
- how effective are the controls to ensure it doesn't happen or happens if it is an opportunity (in terms of design, operation and scope).

Refer to Appendix 2 for ratings to be used when analysing control effectiveness, impact, and likelihood. Refer to Appendix 5 for further understanding of controls.

The Audit Office risk matrix in Appendix 3 is used to determine the level of risk after considering the likelihood and impact of the risk occurring. The same risk matrix is used to determine both the inherent and residual risk ratings. Inherent risk is the level of risk assuming no controls are in place while the residual risk is the level of risk after considering the effectiveness of controls.

Step 2.3: Risk evaluation

Evaluation involves comparing the residual risk rating with the risk appetite (acceptable risk) and determining whether to:

- accept the risk (where it falls within the risk appetite)

  or
- treat the risk (where it is approaching or outside the risk appetite) by applying further mitigating controls or modifying an activity.

For further information about the RAS and tolerances, refer to section 7 above.

9.3 Step 3: Risk treatment

This step involves selecting and implementing options to address the risk, such as:

- adopting further mitigating controls or modifying the activity so that the risk falls within the risk appetite

  or
- ceasing the activity all together if the risk cannot be mitigated to within the risk appetite.

In deciding the risk treatment, the following needs to be considered:

- what options are available to treat the risk
- what are the costs of the treatment compared with the impact on risk
- how effective is the treatment
- the risk velocity - for example, a risk with a velocity of very rapid will require a treatment plan that is in force immediately to contain and minimise the impact of the risk compared with a risk velocity of slow where the treatment plan can be implemented over a longer period. Refer to Appendix 2 for the risk velocity ratings to be used.

9.4 Step 4: Recording and reporting

Risks and risk assessments should be recorded within the Audit Office's risk register and risk reports saved within the Audit Office's records management system.

Risk reporting ensures the communication and sharing of risk information across the Audit Office and is a key mechanism in the management of risks.

The status of risks and reviews of the RMF and its underlying documents must be reported to the Office Executive and ARC on a regular basis as outlined in accordance with the reporting schedule. Refer to Attachment 4 for the risk reporting schedule.

To assist risk owners to prepare reports, a risk reporting template is available. The Office Executive reporting brief template also has a risk section where risks are considered for each decision required by the Office Executive.

9.5 Step 5: Communication and consultation

Risks should be escalated to your manager when one or more of the following situations arises:

- treatment of the risk requires expenditure outside of the risk owner's delegation
- the risk impacts multiple branches or requires the input or action of multiple branches
- treatment of the risk requires a strategic or organisational change such as a policy change
- operating outside or approaching the boundaries of the risk appetite
- a risk is quickly emerging or evolving and has a rapid or very rapid velocity.

Risks should be timely escalated to your manager or higher, depending on the severity and nature.

9.6 Step 6: Monitoring and review

In a continually changing environment, ongoing developments and shift in priorities, risks must be monitored and reviewed regularly. The above steps are to be repeated on an ongoing basis so that emerging risks can be identified, controls remain effective, and opportunities to improve the overall RMF are embraced.

With limited time and resources, monitoring and review activities should be prioritised to focus on the most critical controls and risks.

10. Controls

10.1 What is an internal control?

Controls are measures that maintain and/or modify risks. They aim to reduce the likelihood and/or consequence of a risk.

Controls include, but are not limited to, any process, policy, device, practice or other conditions and/or actions which maintain and/or modify risk.

10.2 Effective internal controls

Effective internal controls help to mitigate risks. 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.

Refer to Appendix 2 on the ratings to be used in assessing the effectiveness of controls.

It is acknowledged that there are inherent limitations of internal controls which include: resource constraints, human judgement and errors, manual and automated controls that can be circumvented by collusion and inappropriate overriding of internal controls by staff or management.

10.3 Control features

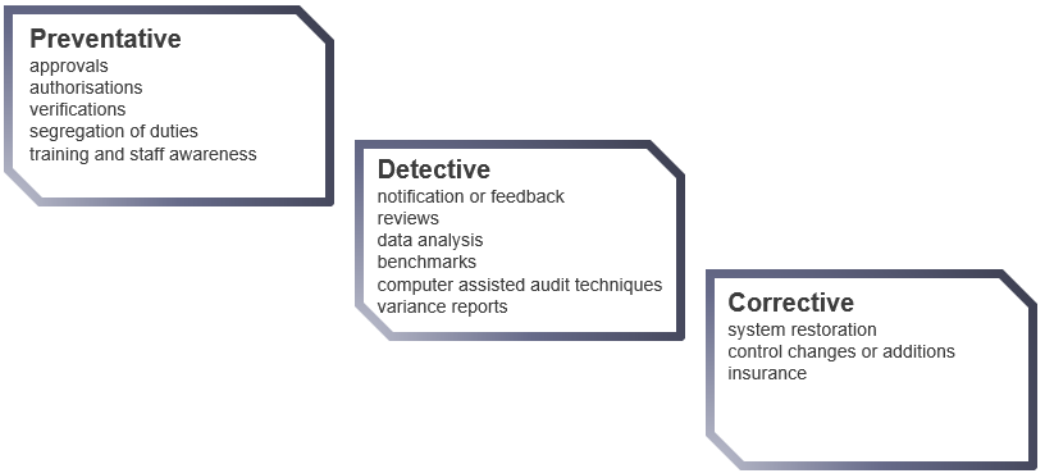
Understanding the features of a control can help to determine the effectiveness of a control. Some controls may not fall distinctly within one category but may have several features. While some controls may be preferred over others, for example preventative over corrective controls, all types of controls have a place when managing risks or taking advantage of opportunities.

Controls can be:

- **manual** which requires human intervention. For example, sighting a security pass to allow physical access.
- **automatic** which does not require any human intervention. For example, a system control preventing a payment without an online approval.
- **combined** which is a mix of manual and automatic controls.

Controls can be classified as:

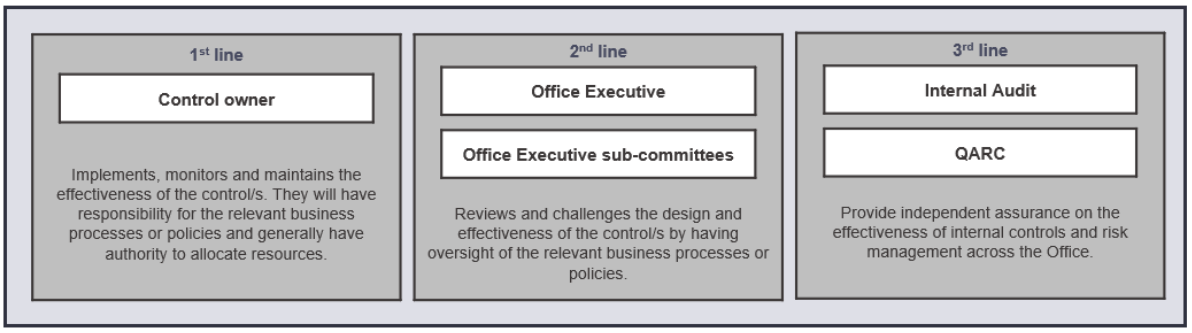
- **preventative** – is a proactive approach which prevents or avoids risk events from occurring.
- **detective** – is a more reactive approach by detecting that a risk event has occurred or identifying control weaknesses.
- **corrective** – is a measure that is implemented to correct problems or issues after they have been identified.



10.4 Control owners and responsibilities

Control owner is the person assigned the responsibility for ensuring the control activity is in place and operating effectively. They are usually the person who has oversight over the controls and generally has the authority to allocate resources. The control owner does not necessarily perform the control and may or may not be the risk owner.

The Audit Office has adopted the Three Lines Model to assign roles and responsibilities in relation to controls.



Refer to section 6.2 for the Three Lines Model used to assign roles and responsibilities for risks.

11. Systems and tools

The RMF includes several key systems and tools as follows:

- risk register
- risk reporting template including OE and ARC brief
- environmental scan
- risk assessment tools – internally developed or externally available tools, as provided on Alfie.

12. Review

To ensure continual improvement, this RMF will be reviewed at least every three years or sooner if any significant new information, legislative or organisational change warrants an update in this document.

Appendix 1 – Definitions

Acceptable risk is the risk rating which is acceptable and comparable to the residual risk. Is equivalent to the risk appetite.

Consequence is the outcome of an event affecting objectives. They can:

- be certain or uncertain and can have positive or negative, direct or indirect effects or objectives.
- be expressed qualitatively or quantitatively.
- escalate through cascading and cumulative effects.

Control is a measure that maintains and/or modifies risk. They may:

- include but not limited to, any process, policy, device, practice or other conditions and/or actions which maintain and/or modify risk.
- not always exert the intended or assumed modifying effect.

Control effectiveness describes how well a control reduces or manages a risk. In assessing control effectiveness, both the design and implementation of the control will need to be considered.

Control owner is the person assigned the responsibility for ensuring the control activity is in place and operating effectively. The control owner does not necessarily perform the control activity but has oversight.

Effect is the deviation from the expected outcome or norm.

Emerging risk is a newly developing or evolving risk.

Event is an occurrence or change of a particular set of circumstances. It can

- have one or more occurrences and can have several causes and several consequences.
- be something that is expected which does not happen or something not expected and which does happen.
- be a risk source.

Inherent risk is the level of risk assuming no controls are in place.

Impact see definition for consequence.

Issue is an event that has already occurred, or is currently incurring, and is impacting, or has had an impact, on objectives. This is compared to a risk which has not occurred.

Key risk indicator is a metric used to provide an early signal of a risk approaching or exceeding risk appetite.

Likelihood is the chance of something happening. Irrespective of whether it is defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).

Mitigation is the measures or actions that affect a change on the impact or the likelihood of a risk event. Interchangeable with risk treatment. When a mitigation or treatment has been deployed as planned it becomes a control.

Operational risk is a risk that may eventuate at the operational or control level while conducting everyday business activities and may prevent operational objectives from being met.

Project risk is a risk that may eventuate within a project that may prevent project objectives from being met. They could include risks relating to project timeframes, budget, output quality, benefits, etc

Residual risk is the level of risk after considering the effectiveness of controls.

Risk is the effect of uncertainty on objectives.

- An effect is a deviation from expected. It can be positive (as in an opportunity), negative or both, and can address, create or result in opportunities or threats.
- Objectives can have different aspects and categories, and can be applied at different levels.
- Risk is usually expressed in terms of risk sources, potential evets, their consequences and their likelihood.

Risk acceptance is an informed decision to accept the consequences and the likelihood of a particular risk.

Risk appetite is the amount of risk an organisation is prepared to accept to achieve its strategic objectives and business plans. It articulates and makes clear the boundaries which the Audit Office is willing to operate in and guides decision making.

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

- Can be formal or informal. Informal are typically undertaken by subject matter experts and decision makers when considering the governance, a decision may require.
- Involves an assessment of risk events to determine required response.

Risk management is coordinated activities to direct and control an organisation with regard to risk.

Risk matrix table is a matrix that facilitates the consistent application, definition, assessment and measurement of the overall risk rating, considering risk likelihood, consequence, causes, control effectiveness and understanding the operating environment. It allows for the prioritisation of assessed risks and the determination of appropriate risk control measures and their importance in managing risk.

Risk owner is the person assigned the lead for the management and oversight of a risk, including completing and reporting on a formal risk assessment for their respective risk/s.

Risk profile is a broad view of the willingness and ability to deal with risks and an understanding of the portfolio of risks exposed to. A risk profile can be determined for an organisation as a whole or can have different risk profile for different areas within the one organisation.

Risk register provides a repository for recording each risk and its attributes, evaluation, and treatments.

Risk source is an element which alone or in combination has the potential to give rise to risk.

Risk tolerance is a more precise way of stating the risk appetite for a given area of activity and defines how the RAS is to be applied in everyday business activities, when making decisions or executing responsibilities or functions. It sets the acceptable level of variation i.e., the boundaries for risk taking expressed as a specific measurable threshold.

Risk treatment see definition for mitigation.

Risk velocity is the time from the initial risk event happening to the point the impact is felt.

Strategic risk is a risk that may eventuate at the strategic level (impacting the overall direction, performance or sustainability of an organisation) and may prevent strategic objectives from being met.

Target risk is the desired optimal level of risk.

Appendix 2 – Likelihood, impact, velocity and control effectiveness ratings

Use the following scale as a **guide** to determine the likelihood of a risk event occurring.

Likelihood	Definition
Almost Certain	Is expected to occur
Likely	Will probably occur
Possible	Might occur at some time as the event is not entirely unusual
Unlikely	Could occur at some time but the event is unusual
Rare	May occur in exceptional circumstances as is very unusual

Note: While it can be useful to measure 'likelihood' in terms of probabilities or frequency within a timeframe, measurements can be different depending on the type of risk being assessed. Hence no quantitative guidance has been provided.

Use the following scale as a guide to determine the impact (consequence) if a risk event occurred.

	Insignificant	Minor	Moderate	Major	Catastrophic
Financial	Is negligible or easily managed within branch budget and resources. Guide < $30k.	Managed within branch budget and resources. Guide $30k - $100k.	Managed through the reallocation of funds and/or resources or reprioritisation of programs within branch budget and resources. Guide $100k - $500k.	Managed through the reallocation of funds and/or resources or reprioritisation of programs within total Audit Office budget and resources. Guide $500k - $1m.	Requires additional external resources. Guide > $1m
Compliance to internal policy or legal obligation	Isolated and minor non-compliance/breach to an obligation. Improvement recommendation made.	Minor non-compliance/breach to an obligation. Minimal correction needed.	Moderate non-compliance/breach to a key or non-key obligation. May involve an internal review.	Systemic or major non-compliance/breach, likely to a key or core obligation. May involve a formal investigation lead by the Audit Office.	Systemic and significant non-compliance/breach, likely to a key or core obligation. May involve an independent inquiry or investigation.
Legal	Incident/dispute which may be resolved through internal process.	Incident/dispute which may be resolved through minimal once off legal advice from the Crown Solicitor.	Moderate incident/dispute which may require some ongoing legal advice from the Crown Solicitor.	Major incident/dispute or multiple incidents/disputes which may require extensive legal advice from the Crown Solicitor or beyond.	Significant incident/dispute or multiple incidents/disputes that result in prosecution or litigation.
Health, safety and wellbeing	None or minimal impact to a physical or mental wellbeing. First aid may be required. No days lost.	Minor and momentary physical or mental distress managed with minimal intervention or support (e.g., visit to GP). Some days lost.	Moderate and short term physical or mental harm/implication or injury, requiring temporary intervention or support (e.g., hospitalisation). Numerous days lost.	Serious and longer-term physical or mental harm/implications or injury, requiring ongoing intervention, treatment or support. Substantial days lost.	Life-threatening injuries, permanent disabilities, severe psychosocial impact or loss of life. Extensive days lost or unable to return to work.
Reputation (internal and external)	None or minimal impact to reputation. No or little attention/dissatisfaction by internal and/or external stakeholder.	Minor impact to reputation. Minor attention/dissatisfaction by internal or external stakeholders. Involving isolated number of internal and/or external stakeholders.	Some damage to reputation. Little media attention or some attention/dissatisfaction by internal or external stakeholders. Involving small cluster of internal and/or external stakeholders.	Major damage to reputation with trust and credibility questioned. Some media attention or major dissatisfaction by internal or external stakeholders. Involving a larger cluster of internal and/or external stakeholders and possibly an increase in staff turnover above expected levels.	Significant damage to reputation with trust and credibility lost. Adverse media attention or significant dissatisfaction by internal or external stakeholders. Involving a majority of internal and/or external stakeholders or staff turnover well above expected levels.
Environment	Little or no impact to the environment. Localised to the source.	Minimal impact to the environment. Localised to the source.	Moderate harm to the environment. Some effect beyond the source.	Major harm to the environment. Wider effect beyond the source.	Significant harm to the environment. Widespread effect beyond the source.
Operations and continuity	Inconvenient or negligible impact to business operations, systems or delivery of audit services.	Minor impact to business operations, systems or delivery of audit service.	Some interruption to business operations, systems or delivery of audit service.	Major interruption to business operations, systems or delivery of audit service.	Not able to perform critical business operations or deliver audit services, or cessation of key or all systems.

Use the following rating as a **guide** to determine the effectiveness of a control.

Control effectiveness	Descriptor	Definition	Likely effectiveness on risk
1	**Ineffective**	Significant control weaknesses. Controls are lacking or poorly designed to treat the root cause/source of the risk and/or do not operate as intended.	The risk is not being managed and is outside the risk appetite. Residual risk is likely to be higher than the acceptable risk.
2	**Partially effective**	Some control weaknesses which could become significant if not addressed. Some controls could be better designed to treat the root cause/source of the risk or could operate more effectively. The existing controls need to be enhanced or additional controls put in place.	The risk is partially being mitigated and may not be within the risk appetite. Residual risk is likely to be on the boundary or just outside of the acceptable risk.
3	**Substantially effective**	Minor control weaknesses. Controls are mostly designed adequately and are largely operating effectively to address the root cause/source of the risk. There may be some improvement opportunities on controls.	The risk is mostly being mitigated within the risk appetite. Residual risk is within or may be approaching the boundary of the acceptable risk.
4	**Fully effective**	Little to no control weaknesses. Controls are designed adequately and are operating effectively to mitigate the root cause/source of the risk. No further improvements needed except continue to monitor the control's effectiveness.	The risk is being mitigated well within the risk appetite.

Use the following rating as a **guide** to determine the velocity of a risk.

Velocity rating	Descriptor	Definition
1	**Very rapid**	Very rapid onset, little or no warning, instantaneous. Impact within a few weeks or hours.
2	**Rapid**	Onset occurs within several months.
3	**Slow**	Slow onset, occurs over a year and beyond.

Appendix 3 – Risk matrix

		IMPACT				
		Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
LIKELIHOOD	**Almost certain**	Low	Medium	High	Extreme	Extreme
	Likely	Low	Medium	High	High	Extreme
	Possible	Low	Low	Medium	High	Extreme
	Unlikely	Low	Low	Low	Medium	High
	Rare	Low	Low	Low	Low	High

Appendix 4 – Risk reporting schedule

Risk report	Frequency	Coordinator	Accountable	Recipient
RMF review	Triennially	Risk Management Function	Auditor-General	Office Executive and ARC
RAS and tolerances	Biennially	Risk Management Function	Office Executive	Office Executive
Annual report including attestation to TPP 20-08	Annually	Risk Management Function	Auditor-General	Office Executive
Environmental scan	Quarterly	Risk Management Function	Office Executive	Office Executive and ARC
Strategic risks	Annually	Governance Manager	Strategic Risk Owner	Office Executive and ARC
Branch risks	Annually	Governance Manager	Branch head	Office Executive and ARC
Fraud and corruption risks	Annually	Director, Governance and Risk	Executive Director Professional Services	Office Executive and ARC
Compliance risks	Annually	Director, Legislation and Assurance	Executive Director Professional Services	Office Executive and ARC
WHS	Annually	Director, People & Culture	Executive Director Corporate, Experience & Strategy	Office Executive and WHS Committee
ISMS	Quarterly	CIO	Executive Director Corporate, Experience & Strategy	Office Executive and Strategic Technology Committee
Cyber risks	Annually	CIO	Executive Director Corporate, Experience & Strategy	Office Executive
Project risks	As required	Manager, Project Assurance and Commissioning	Project Sponsor	Office Executive and ARC
Deep dive review e.g., following a breach	As required	Branch head	Branch head or Deputy Auditor-General	Office Executive