audit office
OF NEW SOUTH WALES

Risk Management Framework

October 2019

INSIGHTS FOR BETTER GOVERNMENT

contents

1 Introduction

The Risk Management Framework outlines the Audit Office's approach to managing risk throughout the organisation. It aims to:

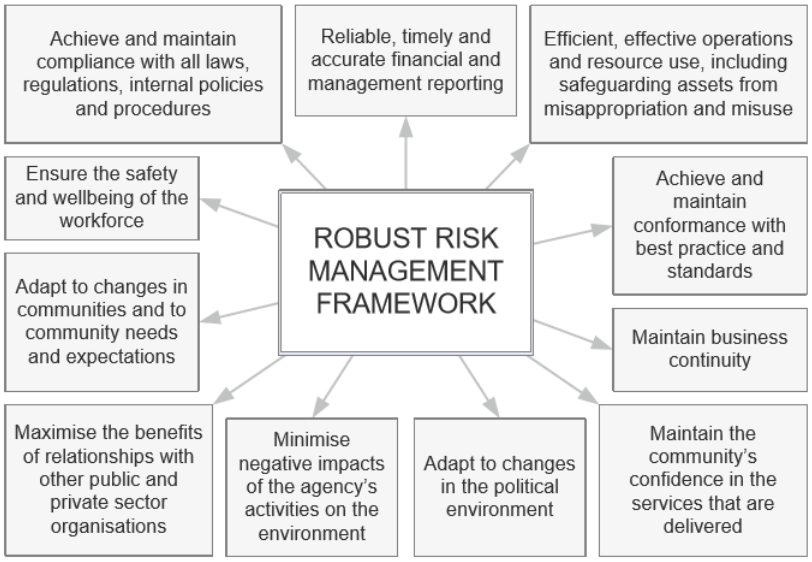
- support effective decision-making
- ensure a consistent and effective approach to risk management while allowing innovation and development
- foster and encourage a risk-aware culture where risk management is seen as a positive attribute of decision-making rather than a corrective measure
- align the Audit Office's planning, quality assurance and risk management systems, and their integration into all areas of the Audit Office's operations.

The framework is integrated with the Audit Office's management systems and processes, corporate planning, performance reporting and key business decisions to implement an enterprise wide risk management approach. The framework is also one of the key eight principles of the Audit Office's Governance Framework, the Governance Lighthouse.

Risk is the effect of uncertainty on business objectives[1]. **The Audit Office's business objectives are outlined in the Audit Office's Corporate Plan 2017–20. The Audit Office's strategic risks are those uncertainties that could prevent the Audit Office from achieving its Corporate Plan, including its vision, purpose and future state**.

Risk management is the culture, processes and structures to identify, assess and manage risk within an organisation. It sets the amount of risk an organisation is willing to take, provides valuable input to strategic and business planning, and should be applied to operations, projects, processes including audit processes, services, and key business decisions.

The Audit Office's risk management framework is developed and maintained in line with the` Management Toolkit for NSW Public Sector Agencies (TPP 12-03) and the Australian and New Zealand Standard AS/NZS 31000:2018 (Risk Management - Guidelines), which provide guidance to agencies on the development of effective and integrated risk management frameworks and processes.



Source: TPP 12-03 NSW Treasury's Risk Management Toolkit for NSW Public Sector Agencies.

[1] AS/NZS ISO 31000 Risk Management – Principles and Guidelines.

2 Components of the Audit Office's risk management framework

2.1 Risk Management Policy

The Audit Office of NSW will establish, implement and maintain an enterprise-wide risk management framework and process that is tailored to achieving the Audit Office's Corporate Plan, meeting business needs and integrated with its systems and processes.

Recognising that the Audit Office generally has a low risk appetite for its core audit activities, the Audit Office will also look to increase its engagement with risk in order to support innovation and a more positive risk management culture and to develop and keep pace within a continuing changing landscape.

Effective risk management requires all Audit Office staff to understand the operational risks and key controls in their areas of responsibility, and actively manage those risks and implement controls as part of their day-to-day activities and decisions. Staff have a role in managing risk and therefore it is important that all staff are familiar with the Audit Office's Risk Management Framework.

In providing independent and professional audit and assurance services to the NSW Government Public Sector, NSW Local Government and Universities, reputational damage is the most critical consequence should our risk management significantly fail. This document communicates the Audit Office's approach to risk management, which includes:

- articulating our risk management policy
- defining our risk appetite and risk tolerances
- developing a positive risk culture where risks are discussed regularly and either accepted or actively managed
- outlining key accountabilities and responsibilities
- articulating our risk management methodology in identifying, assessing and monitoring strategic and operational risks.

The Audit Office will confirm in writing (attest) annually to NSW Treasury as part of the requirements of TPP 15-03 Internal Audit and Risk Management Policy for the NSW Public Sector which includes compliance with the current Standard ISO 31000:2018 Risk management - Principles and guidelines.

2.2 Risk appetite statement and tolerances

The Audit Office's risk appetite is the amount of risk it is prepared to accept to achieve its strategic objectives. Having a documented risk appetite statement:

- allows for a better understanding of our strategic goals, culture, context and sensitivity to risk
- identifies different risk in different parts of the business
- informs the development of risk tolerances for various Audit Office activities and decisions.

The risks to the Audit Office can be significant and a failure to properly manage these risks will impact its ability to deliver its strategic objectives.

Refer to intranet for a copy of the Audit Office's Risk Appetite Statement.

Risk tolerances are the boundaries for risk taking. The risk appetite statement informs the development of risk tolerances for the Audit Office and provides guidance on how the risk appetite statement is to be applied in everyday business activities and decisions.

Refer to the strategic risk register where the determined risk tolerances are captured for each risk.

The following table provides guidance for the relationship between risk appetite, risk tolerance and the adequate risk management approach.

Extent of Risk Appetite	Risk Tolerance Level	Risk Management Approach
High Appetite (Open)		
The Audit Office will operate in this area or in this way after all options are considered and the most appropriate option selected for an acceptable level of reward or value for money. Willingness to take on risk for an acceptable level of reward.	High	Innovate Venture Explore
Moderate Appetite (Acceptable)		
The Audit Office will operate in this area or this way after risks have been effectively mitigated in order to pursue opportunities. This is generally adopted for corporate and management activities. Willingness to take on a moderate level of risk.	Moderate Medium	Confident
Low Appetite (Tolerable)		
The Audit Office may operate in this area or in this way where the value is assessed as worthwhile, and only after risks have been effectively mitigated or uncertainty minimised. This is adopted for core business activities within financial and performance audit and for activities in pursuing key Audit Office strategic objectives. Willingness to take on a limited level of risk.	Limited Low	Conservative
No Appetite (Unacceptable)		
The Audit Office will not operate in this area. No willingness to take on any risk.	Zero	Avoid

2.3 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 entity considers risk in its day-to-day activities. However, the risk culture should be embedded into and not separate from the organisational culture.

Risk culture is the glue that binds all the elements of risk management together, because it reflects the shared values, goals, practices and mechanisms that embed risk into an organisation's decision-making processes and risk management into its operating processes.

At the Audit Office, adopting a positive risk culture is fostered, where risk management is seen as a positive attribute of decision-making rather than a corrective measure. Hence staff must be encouraged to have a willingness to engage effectively with risk.

Actions supporting a positive risk culture at the Audit Office that is conducive to effective risk management includes:

Audit Office Activities	Management Responsibility	Staff Responsibility
Instill shared values and purpose	Provide a **positive tone at the top** - commitment and modelling ethical and responsible behaviour and business decisions. **Allow staff to learn from their mistakes** and being vulnerable to innovation or new ideas.	**Positively engage with risk** within areas of responsibility **Be alert** to potential risks or opportunities
Foster open and upward communication	Have an **open-door policy and open mind** Provide **incentives** – recognise when staff are positively engaging with risk Provide **constructive feedback**	**Confidently escalate** risks, issues, mistakes or opportunities
Adopt a consistent and embedded approach	**Integrate risk management into corporate planning** **Endorse and advocate** the Risk Management Framework **Monitor and review risks and mitigating controls** Provide **adequate resources** with clear risk responsibilities through job descriptions and performance agreements **Ensure business systems and processes are fit for purpose** and commensurate with the risk	**Know your role** Know the risks and implement controls **within your area of responsibility** **Understand the AOs risk management framework**
Promote risk awareness	**Share of knowledge**, learnings and best practice Provide **adequate training**	**Attend risk training** **Learn from mistakes and mentors**

3 Roles and responsibilities

3.1 Auditor-General

The Auditor-General has ultimate responsibility and accountability for the Audit Office's Risk Management Framework.

3.2 Office Executive

The Office Executive is accountable for managing risk in the Office. Members of the Office Executive are also assigned responsibility for specific strategic risks as the risk owner. Risk owners are responsible for ensuring necessary controls and treatment plans are in place to effectively manage that risk including providing adequate resources. Members of the Office Executive are required to attend Audit and Risk Committee meetings as requested to discuss the current management of specific risks.

Audit Directors with key audit responsibility are also responsible to ensure risk based audit methodologies are applied.

3.3 Audit and Risk Committee

The Audit and Risk Committee provides independent assistance to the Auditor-General by monitoring, reviewing and providing advice about the Audit Office's risk management framework and is guided by TPP 15-03 Internal Audit and Risk Management Policy for the NSW Public Sector.

3.4 Chief Risk Officer

The Chief Risk Officer (CRO – Executive Director, Professional Services) is responsible for promoting effective governance and reporting of strategic risks. The CRO must often be the devil's advocate, challenge and offer alternative views to enrich discussions and provide diversity and avoid tunnel vision. The CRO does this with support of the Executive Manager, Governance (Risk) as outlined below.

3.5 Executive Manager, Governance (Risk)

Executive Manager, Governance (Risk) administers and updates the Risk Management Framework including the risk management policy and procedures, maintains the Strategic Risk Register with input from the Office Executive, ensures the annual risk management plan is implemented and co-ordinates detailed strategic and operational risk reports from the risk owners to the Office Executive and Audit and Risk Committee as specified.

3.6 Managers and staff

Managers and staff with key responsibilities such as IT project work, security, work health and safety, financial management and business continuity planning, overseeing projects, managing a business unit, etc. are responsible to ensure that appropriate risk management practice is an integral part of routine business management. This includes identifying, assessing and managing risks within their respective areas of responsibility.

All staff are required to manage risks within the scope of their roles. This means being aware of their team's key risks when making decisions or conducting activities within their area of responsibility and implementing controls to reduce those risks. Staff are also required to support a positive risk culture in the office with responsibilities outlined in the risk culture section above and includes understanding the Audit Office's risk management framework and how it is to be applied.

3.7 Internal Audit

Internal Audit has a role, through its rolling audit program, to review and assess the risk environment and provide insights into risk management, including providing recommendations to improve mitigating actions and controls.

4 Audit Office's risk management methodology

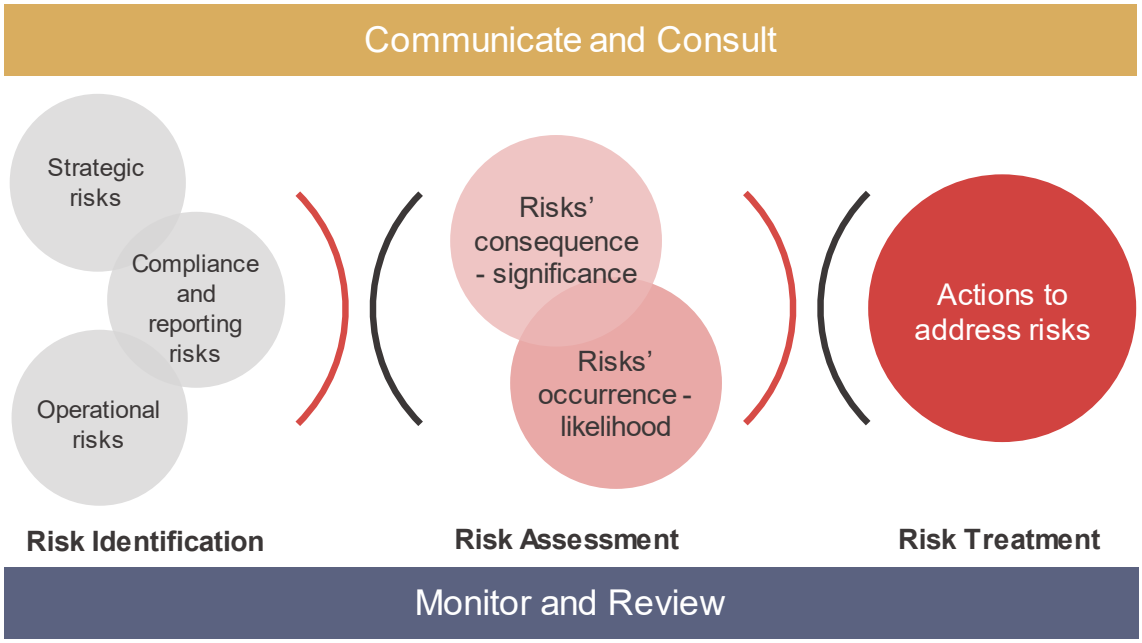
The Audit Office has adopted an enterprise wide and integrated risk management approach. Risks are considered and assessed at different levels within the organisation, across many functions and activities. All risk assessments, including their identification, controls, likelihood, consequence, and residual risk rating should be documented consistently across the Audit Office, using the risk management process described above. Controls embedded within the Audit Office's current business processes are identified as part of the risk evaluation process.

The Audit Office requires that a formal risk assessment be undertaken in all key areas, including when:

- planning and conducting audits
- developing corporate and branch business plans
- assessing specific work health and safety implications or concerns
- conducting significant procurement activities
- undertaking business continuity and disaster recovery planning
- assessing protective security requirements
- key business decisions
- managing projects.

The results should be documented in a risk register using the Audit Office's risk register template or in the case of planning and conducting audits, as prescribed by the audit and assurance policies, procedures and methodology.

An overview of the Audit Office's risk management process is:



4.1 Risk identification

Risks are identified by examining sources of risk, areas of impact, causes and potential consequences of events and scanning the environment. Risks are also identified by the risks associated with not pursuing an opportunity. A list, or register, of risks is generated from the identification process for analysis and evaluation.

4.2 Risk assessment (analysis and evaluation)

Risk analysis involves developing an understanding of an identified risk. This involves:

- identifying the causes and sources of the risk
- identifying and assessing the effectiveness of existing controls to mitigate the risk
- determining the potential consequences and likelihood of the risk occurring.

Through this process the level of residual risk can be determined and is compared with the predetermined risk tolerance in order to decide if further treatment is needed.

4.2.1 Guide to Rating of Existing Controls

Rating	Definition
1	Existing controls are ineffective
2	Existing controls are only working to mitigate a small amount of the risk
3	Existing controls are working to mitigate some of the risk
4	Existing controls are working moderately well to mitigate the risk
5	Existing controls are working well to mitigate the risk
6	Existing controls are working very effectively to mitigate the risk

(A scale of 1 to 6 is used to measure how well the control is working to reduce the risk.)

4.2.2 Risk analysis matrix

The Audit Office uses a risk analysis matrix to determine the level of risk. A risk rating of either extreme, high, medium, or low is used and is dependent on the expected likelihood and impact of the event happening. The same risk matrix is used to determine both the inherent and residual risk rating i.e. before and after assessing the effectiveness of existing controls. The risk matrix is also to be consistently used throughout the Audit Office in assessing both strategic and operational risks.

		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

4.2.3 Selecting Likelihood and Impact

The likelihood and impact rating is informed by experience, judgement, intuition and other relevant information.

Likelihood	Definition
Almost Certain	Is expected to occur in most circumstances based on experience or knowledge
Likely	Will probably occur in most circumstances based on experience or knowledge
Possible	Might occur at some time as the event is not unusual
Unlikely	Could occur at some time as the event is unusual
Rare	May occur in exceptional circumstances as is very unusual

Impact	Level of Impact on Organisation	Operation	Image and Reputation	Financial and Staff Resourcing	Legal and Regulatory Compliance	WHS
Insignificant	Local level (specific area within a business unit)	Little impact. Concerns resolved via standard business practices	Minimal inconvenience to staff, clients or stakeholders	Can be handled within local discretionary budget and resources – Guide <$5k	Failure to comply with internal guidelines	None or only minor personal injury; First Aid needed but no days lost
Minor	Audit Office Business Unit (e.g. CS Unit, Audit teams, Governance)	Inconvenient	Local media attention. Inconvenience to staff, clients or stakeholders	Can be managed within business unit area budget / resources – Guide $5k-$100k	Failure to comply with internal or external guidelines	Minor injury; Medical treatment & some days lost
Moderate	Audit Office Branch	Serious management attention required to resolve concerns	State media attention. Serious inconvenience to staff, clients and stakeholders	Requires reallocation of funds and/or resources or reprioritisation of programs within Audit Office branch – Guide $100k - $250k	Failure to comply with internal and external Audit Office standards and policies	Injury; Hospitalisation & numerous days lost
Major	Whole of Audit Office	Unacceptable interruption to functions	Adverse and extended state or national media coverage. Complaints from staff, clients and stakeholders	Whole Audit Office must redirect significant funds or resources internally – Guide $250k - $2m	Failure to comply with State and Commonwealth Law and regulations	Long-term illness, multiple serious injuries or reportable to Safe Work Australia
Catastrophic	External (e.g. Premier, Parliament)	Not able to perform functions	National ongoing media coverage or demand for government enquiry Complaints from majority of staff, clients and stakeholders	Requires immediate supplementation of funding or resources – Guide > $2m	Failure to comply with constitution	Fatalities or permanent disability or ill-health

4.2.4 Risk evaluation

Each risk is evaluated as either acceptable or unacceptable by comparing the residual risk rating i.e. after assessing the effectiveness of existing controls, with the predetermined risk tolerance (see section 2.3).

Risk Rating v Risk Tolerance	Risk evaluation / Strategy
Risk rating greater than risk tolerance	Unacceptable and further treatment required
Risk rating equal to the risk tolerance	Acceptable and continue to monitor the risk
Risk rating less than risk tolerance	May be unacceptable and reconsider reducing controls and mitigating actions to what is required

A treatment option may not be required for a risk if existing controls are deemed sufficient, it poses a minor risk, is unlikely or the cost of further mitigation is greater than the potential impact of the risk. In this case a commitment to maintain and regularly review existing controls will be an adequate treatment option.

4.3 Risk treatment and escalation

4.3.1 Risk treatment

Risk treatments should reduce a risk to an acceptable level (set by the risk tolerance) through improving or modifying existing controls, or may require the level of activities to be revised if the risk rating is significantly lower than the risk tolerance. Options for treating risks include:

- **avoiding** the risk by stopping the activity or choosing an alternative activity
- **reducing** the risk by removing the source of the risk or implementing further mitigation strategies to change the likelihood and consequences of the risk
- **sharing** the risk with another party
- **accepting** the risk to pursue an opportunity but may include implementing further mitigation strategies.

In selecting the appropriate risk treatment, the risk owner needs to consider such things as the cost and effort of implementing the treatment against the potential benefits, the level of risk (risk rating), and the risk velocity.

The risk velocity is the time from the initial cause or the risk happening to the point the impact is felt. The risk velocity can be measured as:

Rating	Descriptor	Definition
1	**Very rapid**	Very rapid onset, little or no warning, instantaneous. Impact within 72 hours.
2	**Rapid**	Onset occurs within a month or two.
3	**Slow**	Slow onset, occurs over several months and beyond.

So, the treatment plan should match 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.

Treatment plans document the chosen treatment options.

Risk Rating	Strategy
Extreme	Risk managed by an established, tailored controls regime which requires appropriate responsibility at the highest level. Requires frequent, highly focused monitoring and review by experienced personnel. Review at least monthly by the Office Executive.
High	Risk managed by an established, tailored controls regime which requires appropriate responsibility at senior level. Reviewed regularly throughout the year by the Office Executive.
Medium	Risk managed by an established, tailored control regime and reviewed at least annually.
Low	Risk managed by routine controls, some additional treatment may be required.

4.3.2 Escalating risk

The identification and assessment of risks do not occur in isolation, but requires the consideration of risks identified and treated in other areas of the organisation. Any significant risks are to be escalated to your manager to ensure that these are appropriately treated and the residual risk reduced to an acceptable level. This will include significant operational and project risks being escalated to the Office Executive for consideration as a new strategic risk or captured in an existing strategic risk.

4.4 Monitor and review

The Office Executive reviews the Strategic Risk Register at least every four months including an in-depth analysis of each risk, or sooner where needed. A Risk Management Reporting Template has been developed to help risk owners prepare the report.

The Audit and Risk Committee similarly examines the Strategic Risk Register and detailed risk reports for each risk. It also receives a bi-annual risk management status report and reviews the Risk Management Framework annually.

The Governance reviews the risk management policy and provides status reports to the Office Executive and the Audit and Risk Committee as specified.