Administrative Review Tribunal

Risk Management Policy

Document owner	Governance Section	
Document link		
Relevant legislation	Section 16 of the Public Governance Performance and Accountability Act 2013	
Related key documents	Risk Assessment Toolkit Strategic Risk Register Operational Risk Register	
Version	**Commencement date**	**Approved by**
1.0	February 2026	Michael Hawkins AM, Chief Executive Officer and Principal Registrar

Contents

Principal Registrar's foreword

Managing risk is a critical part of our work. It helps us achieve our objectives as outlined in our corporate plan, while meeting our obligations as per the *Administrative Review Tribunal Act 2024 (ART Act)* and the *Public Governance Performance and Accountability Act 2013* (PGPA Act).

The Tribunal's Risk Management Policy (the Policy) describes our approach to risk management. This Policy sets out how we will proactively manage and work with risk, our accountabilities and responsibilities, and the level of risk we are willing to accept to achieve our goals. The Policy, as part of our broader risk management framework, establishes a culture of risk management that is embedded in all that we do, allowing us to be prepared for challenges and to innovate.

Over the coming years we will continue to build the Tribunal's risk maturity, through staff training, the provision of new tools and guidance, and developing a culture where risk is an integral part of all planning and decision-making.

Michael Hawkins AM

Chief Executive Officer and Principal Registrar

1. Introduction

1.1. The Policy applies to all staff and members of the Tribunal. It forms part of the Tribunal's risk management framework and articulates our overall intentions, approach and direction in relation to risk management. Terms in **bold** are further defined in the Glossary at **Appendix A**.

1.2. The Policy supports the Principal Registrar's legislative requirement to establish and maintain appropriate systems of risk oversight, management and internal control for the Tribunal under section 16 of the PGPA Act, and complies with the 9 elements of the *Commonwealth Risk Management Policy*.

1.3. **Risk** is the effect of uncertainty on objectives.

1.4. **Risk management** is the coordinated activities to direct and control an organisation with regard to risk. The benefits of risk management include:

1.4.1. helping us make informed decisions

1.4.2. better identification, evaluation, and management of threats and opportunities

1.4.3. improved accountability, governance and financial management

1.4.4. better understanding and management of complex and shared risks

1.4.5. improved organisational performance and resilience.

1.5. The Policy applies to the management of all types of risk which may arise at the Tribunal. This includes:

1.5.1 **Strategic risks** which relate to the achievement of our objectives as set out in our corporate plan and ART Act. They tend to be broader in scope, longer term and are of particular impact or importance as they can affect the strategic intent of the Tribunal.

1.5.2 **Operational risks** which are risks that can impact the organisation's internal activities. These risks can be specific to a business area or function or have an impact across the Tribunal.

1.5.3 **Project risks** (including program risks) which are managed at the program and/or project delivery and activity level and have the potential to impact project and activity objectives. These risks may be articulated in program and/or project work plans or risk registers.

1.6. This Policy should be read together with other plans and policies that govern specific kinds of risk (for example, the Fraud and Corruption Control Plan). Business areas with functional responsibility for specific kinds of risk should ensure alignment with this Policy as far as is practicable. In the event of an inconsistency with this Policy, the more specific provision prevails

2. Principles

2.1. Risks at the Tribunal must be managed in accordance with the following principles:

- All members and staff have a role in risk management.
- Risk management is integrated into business activities, systems, and decision-making.
- Risk should be the responsibility of those best able to control or manage them.
- Risk management will be applied at both strategic and operational levels throughout the Tribunal to ensure we operate within an environment of continuous improvement.

- The effectiveness of controls is reviewed and confirmed biannually and controls are periodically tested to ensure the identification of significant weaknesses or deficiencies.

2.2. The Tribunal has adopted the principles of risk management in line with the Australian Standard: Risk Management—Guidelines (AS ISO 31000: 2018).

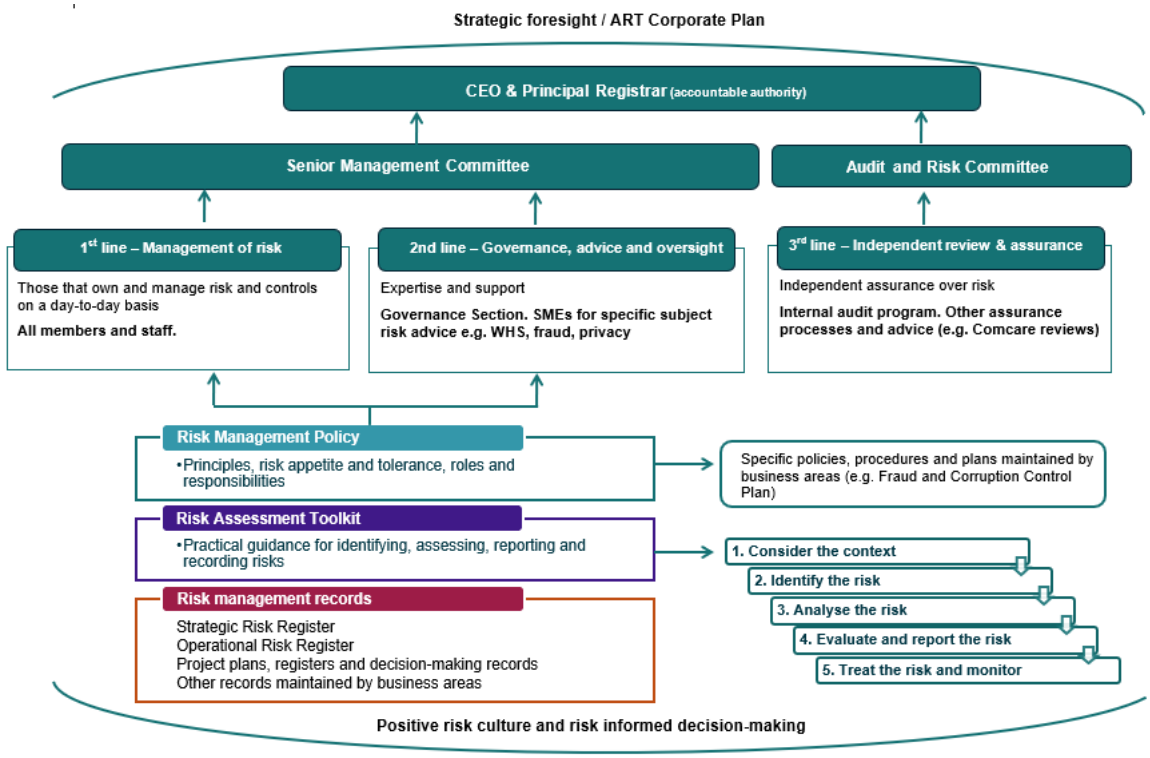
3. Risk management framework

3.1. The Tribunal is required to establish a risk management framework (the Framework) under the *Commonwealth Risk Management Policy 2023.*

3.2. The Framework encompasses this Policy, the Risk Assessment Toolkit, and risk management records. It also includes policies that govern specific kinds of risk such as fraud, and work, health and safety (WHS).

3.3. The Framework is structured along the three lines of defence model which defines roles and responsibilities and is intended to ensure there are no gaps, overlaps or ambiguities in our risk and control activities.

3.4. An overview of the Framework follows:



3.5. The Framework is supported by the Governance Section, who provide risk tools and guidance across the Tribunal, as well as managing the Tribunal's risk management program and training.

4. Responsibilities

4.1. All staff and members are responsible for the day-to-day management of risk in the performance of their duties and responsibilities. This includes identifying, responding and reporting on key risks, and complying with the Framework and the *Commonwealth Risk Management Policy*.

4.2. Roles and responsibilities for risk management across the Tribunal are detailed below:

Official	Responsibilities
Principal Registrar & CEO (accountable authority)	• Responsible for having systems of risk management and oversight in place at the Tribunal, including determining risk appetite and tolerance, and promoting a positive risk culture.
Chief Risk Officer (CRO) (Director, Governance)	• Oversee the Framework and governance for managing risk across the Tribunal, and support the Principal Registrar in understanding the Tribunal's capability to manage risk in line with its risk profile. • Promote risk management practices and culture at the SES level and across the agency, and attend cross-government risk forums as required.
Senior Executive Staff (SES) (including SMC)	• Responsible for reviewing, monitoring and managing risks and controls across the Tribunal and within their branch, including strategic risks through SMC, operational risks, and through branch planning. • Facilitate risk conversations, promote a positive risk culture and embed risk management into the day-to-day decision making process of their branch. • Undertake risk management in decision-making, and promote risk management training and incorporate regular updates regarding risks in their branch.
Audit & Risk Committee (ARC)	• Monitoring and review the appropriateness of the Tribunal's system of risk oversight. • Provide advice to the Principal Registrar on the Tribunal's management of risk and controls, and assurance mechanisms.
Program or project working groups and forums (e.g. Program Control Board)	• Escalation, monitoring and review of the program and / or project(s) risks. • Perform risk owner function, work with program / project managers and risk treatment owners, as required.
Governance Section (including the Director, Governance)	• Responsible for developing and managing the Tribunal's capability to manage risk. • Supporting the CRO and the Principal Registrar meet their duties in regard to risk management, and reporting on risk management to the SMC and ARC. • Provide guidance, training, and tools to assist business areas and staff across the Tribunal to manage risk as per the Framework. • Monitor legislative requirements and best practice risk management, including attending risk management forums.
Risk owners	• Staff with the accountability and authority to identify and manage risks.

Official	Responsibilities
	• Responsible for maintaining effective controls, including assessing their effectiveness and monitoring and reporting on performance. • Report when risks exceed appetite or tolerance and putting in place risk management plans as required.
Control owners (including treatment owners)	• Responsible for maintaining specific controls, implementing treatments and assisting risk owners in assessing control effectiveness and reporting on performance. • Report to the risk owner when a control is no longer effective.
Risk specialists	• Subject-matter experts in relation to particular categories of risk – for example Fraud Officer, Agency Security Advisor, IT Security Advisor or privacy team.
Staff and members	• Responsible for day-to-day management of risks, including managing controls, and reporting where risks exceed appetite.

5. Risk appetite and tolerance

Appetite statement

5.1. The Tribunal provides an important service to members of the community by reviewing a wide range of decisions to afford administrative justice for individuals and organisations and improve government decision-making.

The Parliament and broader Australian community expect us to be a Tribunal of excellence, and we are committed to meeting those expectations and building public trust and confidence in our services.

A risk appetite statement describes the overarching amount and types of risk an entity is willing to accept in order to achieve its objectives. Determining and articulating an entity's risk appetite assists entities to make better choices by considering risk more effectively in decision making.[1]

At the Tribunal we have determined that our overall appetite for risk is **medium**. However, our appetite for risks relating to areas such as the safety of our workforce, legal and compliance and financial loss is **low**.

[1] Element 2: Risk Management Framework | Department of Finance

Tolerance statements

5.2. Our goal is to mitigate all risks to a target risk level of **Medium** or **Low**, where practical and cost effective.

5.3. The following table provides a guide to the preferred target risk levels across categories of risk, and behaviour statements that help or prevent us from achieving those targets.

5.4. If a risk is higher than the target risk tolerance noted below, a risk management plan must be implemented as per the Risk Assessment Toolkit. The risk management plan should follow the escalation and reporting process as per section 8 of this policy.

Risk category	Examples	Target risk tolerance		Risk tolerance statements	We encourage	We discourage
		Low	Medium			
Legal and compliance	Non-compliance with relevant legislation or internal policies or procedures	✓		We have a low tolerance for actions that lead to non-compliance with legislation, policies or procedures. We will not tolerate illegal activities.	A proactive approach to compliance with legislation, internal and external policies and procedures, supported by robust governance arrangements.	Processes, policies, procedures, templates and other tools that are inconsistent or not compliant with applicable legislation. Out-of-date policies and procedures.
Finance and property	Loss, theft, damage of assets, impact on surplus or deficit	✓		We have a low tolerance for risks relating to internal financial loss or damage of assets.	Financial literacy across the Tribunal. Robust procurement processes. Sound financial decisions. Fraud awareness.	Making financial decisions that misalign with our values and are inconsistent with our policies and procedures.
People, culture and integrity	WHS risks, fraud or corruption risks, conduct relating to values / integrity	✓		We have a very low tolerance for risks that impact the health, safety and wellbeing of staff. We will not tolerate fraud, corruption and illegal activities.	Culture aligned with our values, APS values, and the Member code of conduct, and that promotes a positive safety culture.	Not considering the health, safety and wellbeing of our staff, members and stakeholders. Dishonest, corrupt, or illegal behaviour.

Risk category	Examples	Target risk tolerance		Risk tolerance statements	We encourage	We discourage
		Low	Medium			
					Engaged and supportive leadership. Professional development. A speak up culture. WHS conversations.	Activities that erode trust in the Tribunal.
Security, information and technology	Systems, CMS, cyber security, AI	✓	✓	We have a medium tolerance for risks that support innovation and new ways of working through technology. We have a low to medium tolerance for risks relating to systems supporting business requirements (noting that the level of tolerance depends on the nature and purpose of the system). We have a very low tolerance for risks relating to security and information/data management processes (particularly in relation to confidential/personal data accessibility).	Calculated risks towards innovation. Testing new ideas that improve efficiencies and adopting new technology. Continuous review and improvement of systems. Supportive change management practices.	An environment where a fear of failure stymies innovation. Resistance to change. Not considering the needs of the user when making changes.
Service delivery	Services do not meet our standards including accessibility risks.		✓	We have a medium tolerance for risks across our operational areas that impact our ability to deliver services in accordance with our service charter. We have a medium tolerance for risks that support innovation and new ways of working.	Being timely, responsive and accurate. Achieving our purpose and key activities.	Significant delays to the delivery of our services. Impacts to the wellbeing of members, staff and stakeholders.
Stakeholders	Risks associated with liaison arrangements with other agencies, Tribunal users, other third-parties (inc. legal advisory services)		✓	We have a medium tolerance for risks that will assist us in developing and sustaining our stakeholder relationships.	Awareness, empathy, and understanding of our stakeholders and their needs.	Not listening and/or not sharing and using feedback from our stakeholders to improve our services.

6. Risk assessment

6.1. Risks should be assessed in accordance with the Tribunal's *Risk Assessment Toolkit.* Further guidance and templates for managing risk can be found on the Risk management intranet page or by contacting the Governance Section.

6.2. Business areas may adapt the Risk Assessment Toolkit and templates for their own purposes in carrying out their functional responsibilities for certain types of risk.

6.3. An overview of the risk assessment process is as follows:

- **Understand the context** – consider the context including relevant objectives, environmental factors, and the Tribunal's risk appetite and tolerance levels.
- **Identify the risk** – find, recognise and describe risks that may prevent the Tribunal from, or assist us with, achieving any objectives.
- **Analyse the risk** – analyse the nature of risks and their characteristics, including a detailed consideration of uncertainties, risk sources, consequences, likelihood, level of risk, events, scenarios, controls and their effectiveness.
- **Evaluate and report the risk** – compare the results of the risk analysis with the established risk criteria to determine where additional action is required. We immediately report high and critical risks to the SMC via our manager and the CRO.
- **Treat and monitor** – select and implement the most appropriate risk treatment option(s) for addressing risks. We develop and implement risk management plans that include proposed actions, accountabilities and responsibilities, timeframe for completion, resources required and constraints.

6.4. When identifying risks, consideration needs to be given to newly developing or evolving risks (**emerging risks**) and risks that may be shared with other stakeholders (**shared risks**).

7. Recording risks

Risks are recorded in accordance with the table below

Risk type	Register	Description	Review cycle
Strategic	Strategic Risk Register	• Maintained by the Governance Section • Overseen by SMC • This register also captures strategic emerging risks • Shared with the ARC and reported on in the Corporate Plan	Biannual (and as required)
Operational	Operational Risk Register	• Maintained by the Governance Section with input from Risk Owners • Risks are approved by the Risk Owner • Shared with SMC and reported to the ARC	Biannual (and as required)
Project	Program and/or project work plans and planning documentation including risk register	• Maintained by program/project manager • Shared and reported to relevant sponsors, stakeholders and committees as required	As necessary

7.2. Business areas with functional responsibility are responsible for managing any further records required by legislation and risk-specific policies.

7.3. Risks that are no longer material (i.e. the risk is no longer relevant or the risk without controls is of little consequence) then it should be closed in the register to ensure focus remains on material risks.

8. Escalation and reporting

8.1. If you assess a risk as **Medium or above**, you must immediately report the risk to your supervisor. Where the risk is rated **High or Critical** it must also be escalated to the SES level and CRO and a risk management plan prepared where relevant.

8.2. The risk management plan should be approved and monitored by the relevant senior executive.

8.3. New operational risks must be reported to the Governance section for recording in the Operational Risk Register.

8.4. Risks are reported to the SMC via a standing agenda item and quarterly risk reports**...**In the case of critical risks, the Principal Registrar will consider advising the Attorney-General.

8.5. When a risk occurs, check if there is a particular incident reporting process that applies (see table below), otherwise report it to your supervisor or the relevant Risk Owner.

Incident	Reporting process
Cyber security	Cyber security intranet page
Disruption to key business process	Business continuity management
Security or threat/risk of self-harm	Guide to completing a Security Incident Risk or Self-harm Report Threat/Risk of Self-Harm Report Security Risk Report
WHS / workplace issue	Speak up - report a safety issue intranet page Workplace Hazard or Safety Issue Request
Privacy breach	Privacy breaches
Fraud or corruption	Fraud intranet page including Report Fraud information sheet. Fraud risks recorded on the Fraud Risk Register. Corruption intranet page including methods of reporting.
Property damage/loss	Property Management intranet page. Log a Facilities Incident - ART Service Portal

9. Culture, capability and training

9.1. The Tribunal encourages a positive risk culture which aligns with our risk principles and our values. This includes building upon our risk capabilities, taking ownership of risks and controls, and acknowledging good risk management.

9.2. Practical elements underpinning the Tribunal's risk culture, may include:

- regular training on risk management
- risk management advice, tips and reminders in 'Managers messages'
- SES-led risk discussions during branch meetings
- standing agenda item for risk discussions at SMC meetings.
- formal risk reviews as part of the Tribunal's risk reporting process.

9.3. The Tribunal is committed to increasing the understanding and skills of managers and their staff for the application of their risk management accountabilities and responsibilities. This includes encouraging and promoting risk training for all staff, including SES.

9.4. The Governance Section will provide regular guidance and information on risk management to business areas across the agency and maintain the risk management intranet page.

10. Review and assurance processes

10.1. The Framework, including this policy, is reviewed annually or following a significant change in the operating environment.

10.2. Risk management will be considered as part of internal audit activities and a review of the Framework will form part of the regular schedule of internal audits.

10.3. The Tribunal takes part in cross-government assurance programs including the biennial Comcover Risk Management Benchmarking Program (Comcover Survey).

10.4. The performance of the Framework is measured through the results from the Comcover Survey, staff census results and internal audit outcomes.

10.5. The Governance Section is responsible for sharing risk management findings from ANAO audits where relevant with the responsible business area.

Appendix A – Glossary

Control – Any process, policy, device, practice or other action that is in place to regulate or modify the likelihood or consequence of a risk. Controls can be preventative, detective or corrective in nature.

Control or treatment owner – the person or persons who have responsibility for managing a control that mitigates a risk, or implementing a treatment to mitigate a risk.

Emerging risk – A newly developing or evolving risk that could affect the achievement of objectives.

Incident – a risk that has been realised.

Operational risk – A risk that can impact the organisation's internal activities. These risks can have an impact across the Tribunal or be specific to a business area or function.

Program or Project risk – A risk that has the potential to impact programs, projects or activities. These risks may be articulated in program/project work plans or risk registers.

Risk – The effect of uncertainty on objectives. The effect can be a positive and/or negative deviation from the expected outcome. Risk is often expressed in terms of a combination of an event (including changes in circumstances or knowledge) and the associated likelihood of occurrence. It is valuable to note that this definition does not refer solely to negative or down-side risk. It is applicable to both opportunity and threat.

Risk culture – A subset of organisational culture and refers to the system of beliefs, values and behaviours throughout an organisation that shape the collective approach to managing risk and making decisions.

Risk management – Coordinated activities to direct and control an organisation with regard to risk. These activities include the identification, monitoring, communication and reporting of risks.

Risk management framework – A set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.

Risk owner – The person or persons with oversight and responsibility for a risk. This includes assessing the risk and reporting on the risk.

Risk tolerance - The levels of risk taking that are acceptable in order to achieve a specific strategic objective.

Shared risk – A risk where more than one entity (for example other government agencies or external stakeholders) is exposed to or can significantly influence the risk. Shared risks require a collaborative effort of shared oversight and management.

Strategic risk – A risk that relates to the achievement of our objectives as set out in the ART Act and our corporate plan. They tend to be broader in scope, longer term and are of particular impact or importance as they can affect the strategic intent of the Tribunal.

Treatment – the additional action undertaken to treat a risk in response to a risk evaluation where it has been agreed that the risk is outside of the entity's tolerance, the controls in place are ineffective and further mitigation activities are required.