Administrative
Review Tribunal

Risk Assessment Toolkit

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

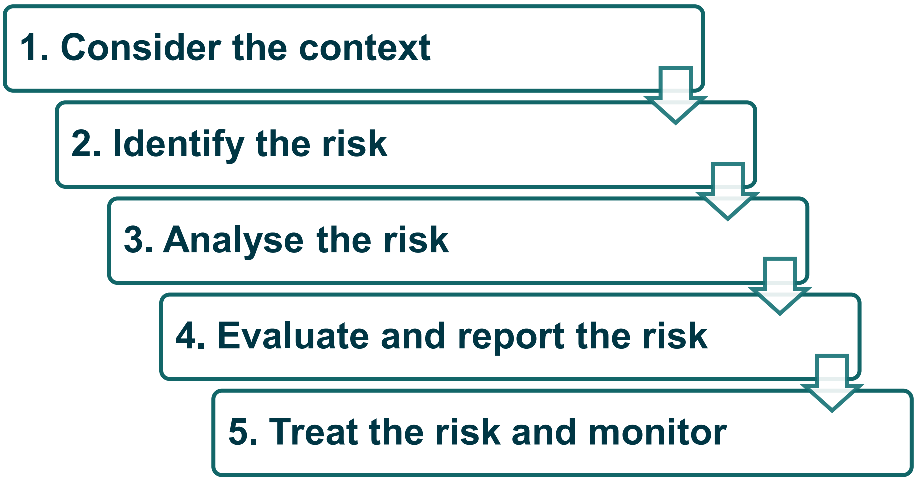
Contents

About this Toolkit

The Risk Assessment Toolkit (Toolkit) forms part of the Administrative Review Tribunal's (Tribunal) Risk Management Framework. It should be read in conjunction with the Risk Management Policy (Policy) and followed when undertaking risk assessments.

The Toolkit aligns with the Australian Standard: Risk Management – Guidelines (AS ISO 3100:2018) and the *Commonwealth Risk Management Policy.*

The Toolkit's purpose is to walk you through the 5 steps of the risk assessment process:



1. Consider the context
2. Identify the risk
3. Analyse the risk
4. Evaluate and report the risk
5. Treat the risk and monitor

Please contact the Governance Section if you require any assistance with reviewing and recording risk, updating the Tribunal's strategic or operational risk registers, or establishing a risk assessment.

Our risk roles and responsibilities

We all have a responsibility to manage risk as part of our day-to-day work and much of this is carried out within the work we do. How we need to formally manage and record risk will depend on our role and the type of risks and controls we are working with, as outlined below:

Role	Risk Assessment Responsibilities	Risk registers input
Staff / Member	• Report changed, new or emerging risks to a supervisor or a Risk Owner • Report if controls are not working or ineffective to a supervisor or Risk Owner • Report incidents or near-misses through relevant channels or to supervisor • Record and assess risks where relevant to work	Where relevant and required (e.g. develop project risk register or a risk management plan)
Risk Owner **(usually EL2s)**	• Identify and manage key operational risks that can impact the Tribunal's key activities • Monitor and maintain effective controls, including assessing their effectiveness and monitoring and reporting on performance.	Operational Risk Register

Role	Risk Assessment Responsibilities	Risk registers input
	- Report when risks exceed appetite or tolerance and putting in place risk management plans as required.	
Control and treatment owner	- Monitor controls and implement treatments. - Report where controls are not working or not effective to supervisor or risk owner - Report when treatment implementation is delayed	Operational Risk Register (via Risk Owner) / Strategic Risk Register (via Governance Section)
Risk specialist / subject matter experts	- Identify and manage specific areas of risk (e.g. fraud, security, WHS, etc) - Monitor and maintain 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.	Specialist risk registers as required.
Senior Executive	- Review, monitor and manage strategic risks through SMC. - Monitor operational risks, program and project risks, and branch planning risks.	Strategic Risk Register

Further information on broader roles and responsibilities for risk management are included in the Policy.

Step 1: Consider the context

When considering your risks, start by understanding the context of the activity including relevant objectives, environmental factors, and the Tribunal's risk appetite and tolerance levels.

Objectives

Consider what you are trying to achieve, at the project and activity level and at the broader operational level. The Tribunal's Corporate Plan and branch plans include useful information on our objectives, environment, and priorities.

Environmental factors

Consider the external and internal environmental context for which the activity operates within.

The external context – this includes policy, operational, cultural, social, political, people, environmental, legal, regulatory, financial, technological and economic factors. Also consider key drivers and trends that impact upon our objectives, and the relationship with, and expectations of, external stakeholders.

The internal context - consider factors within the Tribunal that may impact the achievement of activities including organisational capabilities and culture. Consider factors such as security, information management, WHS, and fraud, and where and how these are managed across the Tribunal.

Risk appetite and tolerance

Consider the Tribunal's level of risk appetite and tolerance, when viewing risk from a threat or opportunity perspective. Refer to the **Policy** for the Tribunal's risk appetite statement, and tolerance levels across six risk categories.

Step 2: Identify the risk

Now that you have considered the context, it's time to find, recognise and describe the risk.

There are various methods of identifying risks. For example:

- brainstorming sessions with staff
- analysing history, lessons learned, near misses (both internal and external to the Tribunal)
- personal or organisational experience
- what-if analyses.

Consider newly developing or evolving risks (**emerging risks**) and risks that we share with other entities (**shared risks**).

When considering risks, use the following Bow Tie analysis method[1] to identify the risk event and its causes and consequences, by writing down the following:

Table 1: Risk identification

The event - what could happen?	**The causes** - what could cause this event to happen?	**The consequences** – what would be the impact of it happening?
E.g. Fraud is committed at the Tribunal	Insufficient fraud controls and checks in place Inadequate segregation of duties, and/or System Access Controls Fraudulent acts occur and are not detected or handled Poor contract management Conflicts of interest are not appropriately identified	Loss of cash, assets and/or information Damage to reputation and criticism of corporate governance arrangements Breach of legislative requirements Loss of trust

What is the risk type?

Determine whether the risk is a **strategic, operational or project risk** (as defined in the Risk Management Policy). This is important for record-keeping purposes.

- Strategic risks are recorded on the Strategic Risk Register in consultation with SMC
- Operational risks are recorded on the Operational Risk Register by the Governance Section. Please contact governance@art.gov.au for assistance

[1] Basic Principles of a Bow Tie Analysis - Protecht AU

- Project risks (including Program risks) are recorded in the relevant program/project management documentation by the program/project owner or manager. A **template project risk register** is available at the end of this Toolkit.

Business areas with functional responsibility for certain types of risk (e.g. People and Culture for WHS) are responsible for managing any specific risk registers and further records required by legislation and policies.

Consult early with the relevant subject matter experts and areas with functional responsibility to ensure alignment with the approach to managing these risks.

What is the risk category?

At the Tribunal we have 6 risk categories for which to assess risks against. A risk might align with one or more of the categories.

Table 2: Risk categories

Risk category	Examples
Legal and compliance	Non-compliance with legislative requirements and obligations or internal policies or procedures
Finance and property	Loss, theft, damage of assets, impact on surplus or deficit
People, culture and integrity	WHS, fraud or corruption, conduct relating to values / integrity
Security, information and technology	Systems, CMS, information, physical and personnel security, cyber security, use of AI
Service delivery	Disruptions and failures to our merits review processes including accessibility risks
Stakeholders	Risks associated with liaison arrangements with other agencies, Tribunal users, other third-parties (including legal advisory services)

Controls

Once you have identified the risk event, causes and consequences, identify the controls that are already in place to mitigate the risk.

When designing or choosing a control it is useful to understand the types of controls and their purpose as this gives an indication of how they work:

- **Detective controls** – detects when something not desired has happened, such as monitoring or exception reporting
- **Preventative controls** – prevents something from occurring or may reduce the severity of the consequences, examples included IT access controls, change authorities, and delegations
- **Responding controls** – reduces the extent of the damage by early intervention or prevents the exaggeration of the consequences

Understanding the type of control is essential for determining whether the control has been designed correctly to address the risk and whether the control is operating effectively. There will also be circumstances in which a spread of detective, preventative and responding controls is needed.

Review of Controls

Controls should be reviewed regularly to ensure they remain appropriate and effective. Control effectiveness is how well a control is reducing or managing the risk that it is designed to modify.

Control effectiveness can be tested through review and assurance mechanisms such as management reviews or internal audit.

Step 3: Analyse the risk

Now that you have identified the controls, it is time to analyse the risk. The purpose of risk analysis is to comprehend the nature of the risk and its characteristics including, where appropriate, the level of risk and how well the controls are managing it.

Assess the likelihood of the risk happening and then the level of impact if the risk does happen.

Use the following tables to determine the likelihood and consequence ratings of the risk.

Table 3: Likelihood rating

Likelihood rating	Description
5 – Almost certain	Expected to occur in almost every circumstance (>90% chance of occurring)
4 – Likely	Considerable opportunity and means to occur (60%-90% chance of occurring)
3 – Possible	Some opportunity and means to occur (40%-60% chance of occurring)
2 – Unlikely	Not expected to occur (10%-40% chance of occurring)
1 - Rare	Almost no opportunity to occur (<10% chance of occurring)

Table 4: Consequence rating

Consequence rating	Legal and compliance	Finance and property	People, culture and integrity	Security, information and technology	Service delivery	Stakeholders
5 – Catastrophic	Non-compliance leading to significant legal consequences and reputational damage. No remediation. Exposure to penalties and criminal liability.	>$1,000,000 Complete loss of infrastructure.	An event causing fatality to one or more persons. Notifiable incident to the WHS regulator, Comcare. Ministerial intervention.	Total failure of critical ICT systems with long term consequences. DDOS or data breach leading to wide scale access to confidential/personal data.	Non-delivery of key Tribunal services for > 1 working day	Significant, long-term damage to relationships with multiple stakeholders affecting the reputation of the Tribunal. Minister loses confidence in the Tribunal.
4 – Major	Non-compliance has occurred leading to legal action and limited remediation is possible. Exposure to penalties.	>$200,000-$1,000,000 Significant damage or loss of property.	Serious injuries causing severe impairment and leading to in patient care at hospital. Notifiable incident to the WHS regulator, Comcare. Systemic fraud or corruption. Significant turnover of staff.	Medium term consequences requiring substantial recovery efforts.	Loss of Tribunal services 1 working day	Significant damage to one or more stakeholder relationships. Many stakeholders lose trust in the Tribunal. Significant and ongoing negative media coverage.
3 - Moderate	Non-compliance has occurred including where part remediation is possible. Warning from regulator or auditor.	>$80,000 - $200,000 Damage or loss of property.	Injuries requiring medical treatment or intervention – typically medical practitioner care. Potentially notifiable incident to the WHS regulator, Comcare. Low level fraud identified. Low staff morale.	Noticeable disruption to operations/partial failure of ICT systems with short term consequences able to be managed internally through DR/business continuity plans.	Loss of Tribunal services 3 -6 hours (during working day)	Damage to relationship with key stakeholders. Some stakeholders lose confidence in the Tribunal. Negative media coverage.

Consequence rating	Legal and compliance	Finance and property	People, culture and integrity	Security, information and technology	Service delivery	Stakeholders
2 – Minor	Non-compliance has occurred which can be remediated.	>$10,000 - $80,000 Minor damage or loss of property.	Reversible injury or illness requiring minimal medical treatment – typically first aid support. Conflicts of interest not managed, workplace values not followed or understood.	Localised, short term disruption leading to minor service delays or inconvenience.	Suspension of services 1-3 hours (during working day)	Minor issue with little impact on the Tribunal's relationship with key stakeholders. Complaints received from stakeholders.
1 - Insignificant	No non-compliance has occurred.	<$10,000 Negligible damage or loss of property.	Incidental workplace incident with no injury or illness. No compromise of workplace values.	No tangible impact to business.	Very minor disruption to services	Very minor issue that does not impact the Tribunal's relationship with its stakeholders.

Step 4: Evaluate and report the risk

Evaluating

Using the likelihood and consequence ratings, you can now evaluate the risk using the matrix below (Likelihood X Consequence = Risk level) and assign it a risk rating.

Table 5: Risk matrix (heat map)

Overall risk rating

LIKELIHOOD

5 **Almost certain**	5 **Medium**	10 **Medium**	15 **High**	20 **Critical**	25 **Critical**
4 **Likely**	4 **Low**	8 **Medium**	12 **Medium**	16 **High**	20 **Critical**
3 **Possible**	3 **Low**	6 **Medium**	9 **Medium**	12 **Medium**	15 **High**
2 **Unlikely**	2 **Very low**	4 **Low**	6 **Medium**	8 **Medium**	10 **Medium**
1 **Rare**	1 **Very low**	**2** **Very low**	3 **Low**	4 **Low**	5 **Medium**
	1 **Insignificant**	2 **Minor**	3 **Moderate**	4 **Major**	5 **Catastrophic**

CONSEQUENCE

Reporting

The risk rating can be compared against our target risk tolerance levels (see the Policy). Depending on the level of risk rating, specific, and sometimes immediate, action may need to be taken. The following table details the actions required for each level of risk rating.

Table 6: Risk reporting

Risk level	Reporting action
Critical Risk rating of 20-25	Report the risk immediately to your manager and Branch Manager and contact the Governance section for advice. The Governance Section will immediately escalate risk to the Chief Risk Officer and Principal Registrar and coordinate urgent briefing to the SMC and the President. Ministerial briefing may also be required. The risk to be recorded or updated in the relevant register and a formal risk management plan with frequent reporting required.
High Risk rating of 15 - 16	Report risk to your manager and Branch Manager, and contact the Governance section for advice. The Governance section to escalate risk to the Chief Risk Officer, coordinate briefing to the Principal Registrar and SMC, and the President where required. The risk to be recorded or updated in the relevant register, and a formal risk management plan with regular reporting required.
Medium Risk rating of 5 - 12	Report risk to your manager. The risk to be recorded or updated in the relevant register and further treatments developed where required.
Low Risk rating of 3 - 4	Dealt with by routine operations with minimal or no treatment. The risk to be recorded or updated in the relevant register if ongoing monitoring of the risk, controls or treatment/s are required. Discuss with the Governance section if required.
Very Low Risk rating of 1 – 2	Dealt with by routine operations within the relevant operations. The risk to be recorded or updated in the relevant register if ongoing monitoring of controls or treatment/s are required. If the risk is no longer material (i.e. it is no longer relevant or without controls, it is of little consequence) then it can be removed.

Step 5: Treat and monitor

Treat

Risk treatment involves choosing what to do about a risk and implementing a strategy of:

- **Mitigation**: Updating controls to modify the likelihood and/or consequence of the risk.
- **Acceptance**: Accepting the level of risk based on informed decision.
- **Avoidance**: Not undertaking the activity.

For critical and high risks, a formal risk management plan must be prepared, which includes:

- Proposed treatments and reasons for treatment selection
- Responsibilities for implementation (i.e. the treatment owner/s)
- Approver (SES level)
- Timing and schedules
- Resource requirements
- Ongoing reporting and monitoring requirements.

A template risk management plan is available at the end of this Toolkit.

Once a risk treatment is implemented, it becomes a risk control. Risk controls are effective if operating in a manner that provides reasonable assurance that processes are consistent and reliable and directed towards the Tribunal's objectives.

Monitor

Risks owners are responsible for ongoing monitoring of the risk, controls and treatments. Monitoring includes detecting changes in the environment involving evolving objectives and ensuring the continued effectiveness and relevance of controls and implementation of risk management plans.

Uncontrollable risks

Not all risks can be mitigated to the desired level of tolerance and not all risks are within our control. It is important to identify these risks, ensure they continued to be monitored and reported on, and focus on consequence management.

Supporting Templates

The following templates are available on the Risk Management intranet site:

- **Risk Management Plan Template** – use this template for the management and monitoring of High and Critical risks, or where a risk requires regular monitoring.
- **Risk Register Template** – use this template for developing risks related to your work, including for programs, projects and section or team plans.