



Toukley Neighbourhood Centre

Ph: 02 43961555 / Email: admin@tnc.org.au / Website: www.tnc.org.au
PO Box 55, Toukley NSW 2263 / ABN: 64 997 484 484 / Association No: Y02437-47

TNC is the heartbeat of a connected, supported, empowered, inclusive and thriving community. We partner with the broader community to share what we can and provide a hand up to those in need, so they can Wallamba-bayn (come back) and join us in delivering our vision.

POLICY – RISK MANAGEMENT

1. Policy Information

Title:	Risk Management
Effective Date:	08-Dec-2025
Policy Owner:	Chairperson, Board of Management
Oversight:	R&CC
Next Review Date:	Dec-2025

1.1. Definitions

This policy uses the terms defined in the *TNC Master Definitions Table*, available on the Toukley Neighbourhood Centre website (www.tnc.org.au/policies).

Policy-specific definitions are listed below (if required).

Term	Explanation
Risk	The possibility that an event, action, or decision will negatively affect TNC's objectives, people, operations, reputation or compliance.
Risk Category	The categories used to classify risks in the Risk Register (HR, Operational, Organisational, WHS).
Risk Appetite	The level of risk TNC is willing to accept in each risk category.
Risk Owner	The role responsible for managing and monitoring a risk.
Control	A measure that reduces the likelihood or impact of a risk. All controls are documented in the Control Register.
Control Owner	The role assigned responsibility for implementing and reviewing a control.
Treatment	An action required to reduce risk to within appetite. Treatments are documented in the Treatment Register.
Treatment Owner	The role responsible for completing treatment actions within required timeframes.
Incident	Any event or near miss indicating that a risk has materialised or may materialise. All incidents are recorded in the Incident Register.

1.2. Context

At Toukley Neighbourhood Centre (TNC), policies are developed in alignment with the *TNC Policy Framework* and support the delivery of safe, effective and accountable community services.

TNC policies are developed to:

- Assist TNC to meet its organisational objects and manage risk effectively
- Support staff and volunteers in performing their duties
- Demonstrate how TNC meets its governance, compliance and quality expectations
- Provide clarity, transparency and consistency across all areas of TNC operations.



This policy must be read in conjunction with the TNC Risk Management Handbook, which provides detailed guidance on risk methodology, scoring, and operational procedures.

TNC is bound by the [Australian Charities and Not-for-profits Commission Act 2012 \(Cth\)](#) and regulated by the [ACNC](#).

Risk information is managed through TNC's integrated digital Risk Framework, including the Risk Register, Control Register, Treatment Register and Incident Register.

1.3. Related Documents

- Risk Management Handbook
- Compliance Policy
- Incident Management Policy
- WHS Framework
- Privacy and Data Protection Policy
- Records Management Procedure.

1.4. Change Control

Effective Date	Author	Approver	Comments
13-Feb-2023	Bronwyn Evans	BoM	Initial document
09-Dec-2024	Bronwyn Evans	BoM	Incorporate definitions for Likelihood and Consequences. Update Risk Categories.
08-Dec-2025	Bronwyn Evans	BoM	<ul style="list-style-type: none"> Updated to new policy template. Aligned to the digitised Risk Framework architecture and technology. Aligned to the new Risk & Compliance Committee structure, Terms of Reference, and accountabilities. Incorporated revised approach to compliance obligations and linkage to the Compliance Policy. Simplified the risk matrix from 4×4 to 3×3 and updated assessment methodology.

1.5. Contents

1.	<i>Policy Information</i>	1
1.1.	<i>Definitions</i>	1
1.2.	<i>Context</i>	1
1.3.	<i>Related Documents</i>	2
1.4.	<i>Change Control</i>	2
1.5.	<i>Contents</i>	3
2.	<i>Policy Overview</i>	4
2.1.	<i>Purpose</i>	4
2.2.	<i>Overview</i>	4
2.3.	<i>Scope</i>	4
3.	<i>Policy Principles</i>	5
	<i>Principle 1: Risk appetite is defined for each risk category.</i>	5
	<i>Principle 2: Risk tolerance determines when treatments are required.</i>	5
	<i>Principle 3: Risk management is integrated with governance, planning and decision-making.</i>	5
	<i>Principle 4: Risks, controls and treatments must have clearly assigned roles.</i>	5
	<i>Principle 5: The Oversighting Committee provides governance oversight on behalf of the BoM.</i>	5
	<i>Principle 6: Risks, controls, treatments and incidents must be reported and reviewed regularly.</i>	5
	<i>Principle 7: Risk management is continuous and proactive.</i>	5
4.	<i>Roles and Responsibilities</i>	6
4.1.	<i>Overview</i>	6
4.2.	<i>RACI</i>	6
5.	<i>Policy Guidelines</i>	8
6.	<i>Processes</i>	9
6.1.	<i>Risk Management Processes</i>	9
6.2.	<i>Recordkeeping Requirements</i>	10



2. Policy Overview

2.1. Purpose

This policy sets out TNC's approach to identifying, assessing, treating, monitoring and reporting risks. It ensures that risks across all areas of TNC's operations are managed consistently, transparently and in alignment with the Risk Management Framework and organisational governance requirements.

2.2. Overview

TNC recognises that risk is inherent in the delivery of community programs and services. Effective risk management supports safety, service quality, financial sustainability, compliance and organisational resilience.

TNC maintains an integrated digital Risk Framework consisting of the Risk Register, Control Register, Treatment Register and Incident Register. These tools support consistent assessment, proactive monitoring, decision-making and escalation.

Risks are assessed using a simplified 3×3 matrix based on likelihood and impact. This provides a consistent methodology for evaluating risk, determining treatment requirements and ensuring risks remain within TNC's approved appetite.

Risk information is reviewed monthly by the Oversighting Committee and reported to the BoM. The EO administers the Risk Framework and ensures risks, controls, treatments and incidents are accurate, up to date and appropriately monitored.

This policy must be read in conjunction with the TNC Risk Management Handbook, which provides detailed descriptions of methodology, scoring, appetite, tolerance, controls and treatments.

There is no circumstance under which risks may be unmanaged, unrecorded or ignored.

2.3. Scope

This policy applies to all TNC staff, volunteers, contractors, students, and any other individuals engaged in TNC activities.

It applies to all TNC programs, services, premises, digital systems, equipment and activities unless otherwise stated within this policy.

Policy-specific scope requirements or exclusions are detailed below (if applicable).

- identification, assessment and documentation of all risks in the Risk Register
- implementation and review of controls in the Control Register
- documentation, monitoring and completion of treatments in the Treatment Register
- documentation and review of incidents in the Incident Register
- application of the 3×3 risk matrix
- monthly monitoring and reporting through the Risk Framework.

3. Policy Principles

Policies always contain a set of principles that provide information relating to the rationale for the document. Staff and volunteers must consider and comply with these guiding principles when performing their duties.

Principle 1: Risk appetite is defined for each risk category.

Risk appetite is approved by the BoM and sets the level of risk TNC is willing to accept across HR, Operational, Organisational and WHS risks.

Principle 2: Risk tolerance determines when treatments are required.

Where a risk exceeds appetite, treatments must be developed, recorded, resourced and monitored until the risk is restored to within tolerance.

Principle 3: Risk management is integrated with governance, planning and decision-making.

Risk information informs strategic planning, program development, budgeting, policy review and organisational improvement activities.

Principle 4: Risks, controls and treatments must have clearly assigned roles.

Risk Owners, Control Owners and Treatment Owners must ensure their assigned risks and actions are accurate, up to date and monitored.

Principle 5: The Oversighting Committee provides governance oversight on behalf of the BoM.

The Committee reviews the Risk Framework monthly, monitors risk trends and overdue items, and escalates material issues to the BoM.

Principle 6: Risks, controls, treatments and incidents must be reported and reviewed regularly.

Risks are reviewed and reported monthly through the digital Risk Framework to support timely visibility, assurance and action.

Principle 7: Risk management is continuous and proactive.

Risks and control performance must be updated in real time, informed by incidents, observations, emerging issues and environmental changes.

4. Roles and Responsibilities

4.1. Overview

Clear roles and responsibilities ensure that TNC policies are implemented effectively, monitored appropriately and aligned with governance expectations.

Accountability for policy application is shared across the organisation, with oversight provided by the designated committee identified in the Policy Information section.

The roles below outline who is responsible for complying with, implementing, and monitoring this policy. Specific responsibilities are clarified further through the RACI table.

Effective risk management requires accurate identification, documentation, assessment and monitoring of risks across TNC. All risks must be recorded in the Risk Register, assigned a Risk Owner and assessed using the 3x3 matrix.

The EO administers the Risk Framework and ensures registers remain accurate, controls and treatments are reviewed, and incidents are recorded and escalated as needed.

Risk Owners monitor risks within their areas, complete assessments, review controls, and ensure treatments are developed and progressed where risks exceed appetite.

Control Owners are responsible for implementing and reviewing controls assigned to them, and reporting weaknesses or overdue reviews.

Treatment Owners complete assigned treatment actions within required timeframes and update progress in the Treatment Register.

The Oversighting Committee provides governance oversight, reviewing risks, treatments, controls and incidents each month and escalating material matters to the BoM.

All staff and volunteers contribute to risk management by identifying hazards, reporting incidents, and following established controls and procedures.

4.2. RACI

This RACI identifies who is **Responsible (R)**, **Accountable (A)**, **Consulted (C)** and **Informed (I)** for the activities required under this policy.

Activity	BoM	Oversighting Committee	EO	Program / Volunteer Coordinators	Staff and Volunteers
Generic Policy Activities					
Understand and comply with the policy	I	I	C	R	R
Implement policy requirements in daily operations	I	I	A	R	R
Maintain procedures and records required by the policy	I	I	A	R	R
Monitor compliance and identify issues	I	A	R	R	R
Report incidents, risks or non-compliance	I	C	A	R	R
Review policy effectiveness and recommend improvements	I	A	A	C	I
Approve policy revisions	A	C	R	I	I

Activity	BoM	Oversighting Committee	EO	Program / Volunteer Coordinators	Staff and Volunteers
Policy Specific Activities					
Maintain the Risk, Control, Treatment and Incident Registers	I	A	R	C	I
Identify and record risks within areas of responsibility	I	C	A	R	C
Assess risks using likelihood and impact scales	I	A	R	C	C
Review controls and complete scheduled control reviews	I	A	R	C	C
Develop treatments for risks that exceed appetite	I	A	R	C	I
Monitor treatment progress and update the Treatment Register	I	A	R	C	I
Escalate risks, incidents or overdue actions	I	A	R	C	I
Review risk performance, trends and emerging issues monthly	I	A	R	C	I
Report the organisation's risk profile to the BoM	I	A	R	I	I

5. Policy Guidelines

The policy guidelines outline the rules, expectations and minimum requirements that must be followed under this policy. These guidelines apply to all individuals covered in the Scope section and support consistent, safe and compliant delivery of TNC operations. Policy-specific guidelines are listed below.

- All risks must be recorded in the Risk Register and maintained in accordance with the Risk Management Framework.
- Risk assessments must use the 3×3 likelihood and impact scales and be reviewed regularly.
- Every risk must have an assigned Risk Owner responsible for monitoring and updating the risk.
- Risks that exceed appetite must have treatments documented in the Treatment Register, with clear due dates and assigned Treatment Owners.
- Controls must be implemented, reviewed and documented in the Control Register by assigned Control Owners.
- All incidents must be reported and recorded in the Incident Register and reviewed in line with the Incident Management process.
- Risks, controls, treatments and incidents must be reviewed monthly through the digital Risk Framework.
- Emerging risks, overdue items or concerns must be escalated promptly to the EO and the Oversighting Committee.
- Risk information must be used to inform planning, budgeting, policy review and program delivery.
- Records supporting risk decisions (evidence, assessments, reviews, discussions) must be retained in accordance with records management requirements.

6. Processes

The processes describe how the requirements of this policy are applied in practice. They outline the key steps, actions and records needed to implement the policy effectively. Detailed procedures or work instructions, where required, are maintained separately and referenced from this section.

6.1. Risk Management Processes

Risk Identification

- Identify risks arising from programs, operations, people, facilities, finances, information, governance, or external factors.
- Record risks in the Risk Register with a clear description and assigned Risk Owner.
- Update risks promptly when circumstances change or new risks emerge.

Risk Assessment

- Assess risks using the 3×3 likelihood and impact scales from the Risk Management Handbook.
- Ensure scoring reflects current information, incidents, control performance and environmental factors.
- Compare the calculated rating to approved appetite for the relevant risk category.
- Document rationale for the rating when required.

Control Management

- Implement controls assigned to each risk and document them in the Control Register.
- Control Owners complete scheduled control reviews and record outcomes, including control performance, gaps or failures.
- Report weaknesses, overdue reviews or resourcing issues promptly.

Treatment Planning and Monitoring

- Where risks exceed appetite, develop treatment actions to reduce likelihood or impact.
- Document treatments in the Treatment Register with due dates and assigned Treatment Owners.
- Treatment Owners update progress regularly and escalate resourcing or timing risks promptly.
- EO and Oversighting Committee monitor overdue or stalled treatments and ensure appropriate action is taken.

Incident Management

- Record incidents, near misses and emerging issues in the Incident Register.
- Ensure linkage between incidents and associated risks or controls where relevant.
- Review incident trends monthly to inform reassessment and treatment needs.

Monthly Review and Reporting

- EO ensures risks, controls, treatments and incidents are reviewed monthly through the digital Risk Framework.
- Oversighting Committee reviews:
 - ◆ changes in risk ratings
 - ◆ overdue treatments or control reviews
 - ◆ new or emerging risks
 - ◆ incident trends
- Monthly reports to the BoM provide a consolidated view of risk status, exceptions and required decisions.

Annual Review

- Conduct an annual review of the Risk Framework, including methodology, scoring, risk categories, appetite, governance arrangements and reporting.
- EO documents findings and presents recommendations to the Oversighting Committee and BoM.

Integration with Governance

- Use risk information to support strategic planning, budgeting, policy development and quality improvement.

- Ensure obligations arising from legislation, contracts, WHS, privacy or internal policies are recorded and monitored through the Compliance Policy.

6.2. Recordkeeping Requirements

Records created under this policy must be stored in accordance with TNC's records management requirements. This includes ensuring records are complete, accurate, accessible to authorised personnel, and retained for the required period.

Records may include:

- risk assessments and updates
- control descriptions and control review records
- treatment actions and progress updates
- incident reports and associated analysis
- monthly R&CC and BoM risk reports
- annual risk review documentation.