

Risk Management Policy

Date Adopted 18 November 2025

Version: 3

Policy Objectives

The objective of this policy is to articulate Council's commitment to implementing integrated risk management principles, systems and processes ensuring the consistent, efficient, and effective assessment of risk in all of Council's planning, decision-making and operational processes.

Policy Scope

This policy applies to all Staff, Councillors, Contractors, Volunteers of Council in its planning, decision-making and operational processes, and supports the strategic goals and objectives that it seeks to achieve on behalf of the Maitland community.

Risk management is integrated into Council's Integrated Planning and Reporting Framework, including the Community Strategic Plan, Delivery Program and Operational Plans. This ensures that risks are identified and managed in a way that supports the delivery services, achievement of strategic outcomes and long-term sustainability for the community.

Policy Statement

Risk management plays a key role in ensuring that Council achieves its objectives. Council understands the internal and external risks that may impact the obtainment of objectives and has processes in place to identify, mitigate, manage and monitor those risks to ensure the best outcome for Council, staff and the community.

Taking a structured approach to the management of risk throughout the organisation, will promote and demonstrate good corporate governance, to minimise loss and maximise opportunities to improve service delivery, consistent with Australian Standard ISO:31000.

Council is committed to the principles, framework and processes of managing risk as outlined in ISO:31000 and commits to fully integrating risk management within Council and applying it to

decision-making, functions, services and activities, in accordance with statutory requirements. In managing risk, Council relies on the three lines of defence approach.

1. The First Line of Defence: Managers, Team Leader, Co-ordinators and Staff- responsible for ownership and management of departmental risks and implementing corrective actions to address process deficiencies. Controls are designed into systems and processes under their guidance.
2. The Second Line of Defence: Risk management and compliance functions - ensure risk management is embedded across the organisation and monitors first line controls. Facilitate and

monitor implementation of effective risk management practices and assist risk owners in defining risk exposure and reporting.

3. The Third Line of Defence: Internal Audits and External Auditors – Internal Audit provides independent assurance on the effectiveness of governance, risk management, and internal controls. External Audit is under the auspice of the NSW Auditor-General. The audit functions provide Council, senior management and the community with comprehensive assurance, based on the highest level of independence and objectivity.

Council's risk management approach supports the delivery of the Community Strategic Plan, which reflects current and future aspirations of the community. The Plan is built around for strategic directions Let's connect with each other, Let's create opportunities, Let's live sustainably and Let's lead together. By managing risk effectively, Council can make informed decisions that contribute to achieving the community's long-term goals, when there is uncertainty

Responsibilities

Council aims to create a positive risk management culture where risk management is integrated into everyday activities and decision making. It is the responsibility of every staff member and business area to observe and implement this policy and Council's risk management framework:

- Governing Body – Councillors - Demonstrate strategic commitment of risk management including direction in setting Council's risk appetite and risk tolerances, as per Section 223 Local Government Act. Responsible for applying the risk appetite statement to strategic planning and all decision making.
- General Manager - Implementation and effective operation of integrated risk management to the whole organisation, supported by policy, procedures, allocation of adequate resources.
- Executive Leadership Team - Driving risk management across the organisation and implementing the effective operation of risk management within respective areas of responsibility/accountability. Ensuring allocation of appropriate resources for the management of risk. Responsible for applying the risk appetite statement to strategic and operational planning and all decision making.
- Managers - Promote and maintain an environment where managing risk is accepted as the responsibility of each employee. Ensuring all staff have the appropriate capability to perform their risk management roles
- Risk and Insurance Team - Provide technical risk management support and or advice to all Maitland City Council staff, Councillors, volunteers, contractors and other stakeholders as and when required.
- Employees - Being familiar with and understanding the principals of risk management, including complying with all policies, procedures and practices relating to risk management.
- Risk Owners - Responsible for applying Council's risk appetite statement when identifying and considering risks and opportunities associated with decisions they make.
- Audit, Risk and Improvement Committee (ARIC) - The Audit, Risk and Improvement Committee (ARIC) is to provide the Governing body (Councillors) and General Manager with information and

recommendations for improvements on Council’s risk management, documentation, plans and processes, if necessary, as per section 428A of the Local Government Act 1993.

- Internal Audit - Internal auditor forms a part of management’s internal control system and has an advisory role to support the Audit, Risk and Improvement Committee.
- External Audit - Statutory function that provides an opinion on Council’s annual financial reports, as required under Divisions 2 and 3 of the Local Government Act 1993, to Council and its external stakeholders.

Policy Definitions

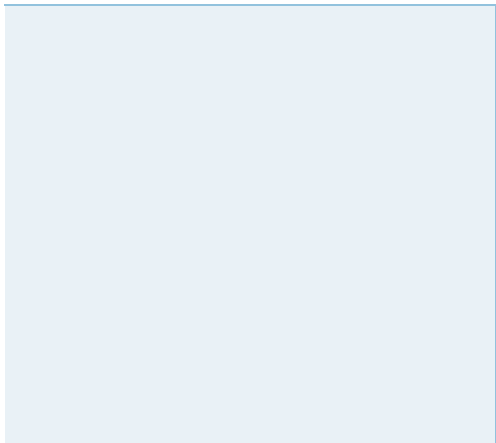
TERM	MEANING
Risk	Is defined as “the effect of uncertainty on objectives”. An effect is a deviation from the expected. The effect can be positive, negative or both, and can address, create, or result in opportunities and threats
Risk Management	Is defined as the “coordinated activities to direct and control an organisation about risk”
Risk Management Framework	A set of components that provide the foundations, framework and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation. It will also indicate how risk management will be integrated within/across the organisation
Risk Appetite	Is defined as the “amount and type of risk that an organisation is willing to pursue and retain”
Stakeholder	Is defined as “a person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity”
Strategic Risk	Is defined as “uncertainties that may arise affecting the achievement of strategy and business objectives”
Operational Risk	Is defined as “uncertainties that may arise in the course of conducting daily business activities, procedures and systems”
Audit, Risk and Improvement Committee (ARIC)	In accordance with “section 428A of the Local Government Act 1993, the role of the Committee is to review and provide independent advice to the Governing Body and General Manager regarding the aspects of Councils operations”

Monitoring and Review

Council is committed to continually improving its ability to manage risk. Council will review this policy every 3 years from date of adoption. to ensure it continues to meet the requirements of the Local Government Act 1993, Local Government (General) Regulation 2005, and Council’s requirements.

Policy Administration

Business Group:	People and Performance
Responsible officer:	Executive Manager People and Performance
Council reference:	Item 14.1 – Council Meeting 18 November 2025
Policy review date:	Three (3) years from date of adoption
File number:	81/17
Relevant legislation	<ul style="list-style-type: none"> • NSW Local Government Act 1993 (including S428a) • Local Government (General) Regulations 2005 NSW Local Government (General) Amendment (Audit, Risk, and Improvement Committees) Regulations 2023 • Work Health and Safety Act 2011 and Regulation 2017 • Environmental Planning and Assessment Act 1979 • Roads Act 1993 • State Records Act 1998 • Civil Liability Act 2002 • ISO 31000:2018, risk management principles and guidelines
Related documents	<ul style="list-style-type: none"> • Audit, Risk and Improvement Committee Terms of Reference • Internal Audit Charter and Plan • Maitland City Council Work Health and Safety Policy & Procedures • Statewide Mutual best practice manuals and guidance material including Continuous Improvement Pathway Workbooks • Statewide Mutual/Marsh Risk Appetite Statements Report May 2024 • Maitland City Council – Risk Management Policy 81/1 • Maitland City Council – Enterprise Risk Management Strategy



- Enterprise Risk Management Framework
- Maitland City Council – Enterprise Risk Management Risk Appetite Statements
- Maitland City Council – Enterprise Risk Management Plan
- Maitland City Council – Risk Assessment Guide
- Maitland City Council – Strategic Risk Register
- Maitland City Council – Operational Risk Register

Policy History

VERSION	DATE APPROVED	DESCRIPTION OF CHANGES
1.0	28 April 2015	Development of new policy
2.0	25 July 2022	Policy reviewed and amended to reflect changes including, ISO 310000, changes to section 428A Local Government Act 1993, incorporating the Audit, Risk and Improvement Committee
2.1	12 February 2025	Updated to new branding and alignment to organisation structure. No change to content
3.0	18 November 2025	Policy reviewed and amended for common terminology across MCC Enterprise Risk Management documentation, update of review frequency to align with Enterprise Risk Management framework