

# Draft Enterprise Risk Management Policy

---

MSC12E

Authorised by:	Internal/External:	External
Date:	Minute No:	
Review timeframe:	4 years	
Review due date:		
Department:	Governance and Risk	
Document Owner:	Manager Governance and Risk	

# Table of Contents

1. Policy Objective .....	3
2. Risks being addressed .....	3
3. Scope .....	3
4. Definitions .....	3
5. Policy Statements .....	5
6. Roles, Responsibilities and Delegations.....	5
7. Dispute Resolution.....	6
8. Related Documents .....	6
Legislation and Guidelines .....	6
Other Supporting Documents.....	6
9. Version History.....	6

DRAFT

## 1. Policy Objective

The purpose of this Policy is to formalise Muswellbrook Shire Council (Council)'s commitment to effective Risk Management practices that support the achievement of its Strategic and Operational Objectives.

Risk Management enables Council to make informed decisions, improve performance, protect community assets, and enhance public trust in service delivery.

This Policy provides the foundation for ensuring that Risk Management is integrated into the overall culture of the organisation with a consistent and structured approach to identifying and managing risk across all areas of Council's operations.

## 2. Risks being addressed

This Policy addresses the key categories of risk that may impact Muswellbrook Shire Council's ability to achieve its strategic, operational, and community objectives. These risks are defined in the Council's Risk Taxonomy within the Enterprise Risk Management Framework, and include governance and reputation, strategic planning, financial sustainability, people and culture, work health and safety, service delivery, environmental management, technology and cybersecurity, and legal and regulatory compliance.

By addressing these risks, the Policy provides a structured and consistent foundation for informed decision-making, enabling Council to proactively manage threats and opportunities that may influence its performance, service delivery, and long-term resilience.

Council recognises that risks may arise from both internal and external sources, and that an integrated and forward-looking approach to risk management is essential to supporting strong governance and protecting public value.

## 3. Scope

This Policy applies to all areas of Muswellbrook Shire Council's operations, including Elected Members, the General Manager, all Council staff, volunteers, and contractors. It is relevant to Strategic, Operational, Project, and Compliance activities, and applies to all functions, services, and decision-making processes.

## 4. Definitions

The following definitions are provided to support consistent understanding of key terms used throughout Muswellbrook Shire Council's Enterprise Risk Management Policy and the Enterprise Risk Management Framework.

These terms are essential to interpreting the Council's approach to identifying, assessing, managing, and monitoring risk across all functions and activities.

Term	Definition
Risk	Effect of uncertainty on objectives (can be positive, negative or both and can address, create or result in opportunities or threats)
Enterprise Risk Management (ERM)	A structured and integrated approach to identifying, assessing, and managing risk across the organisation to support informed decision-making, accountability, and performance.
Risk Appetite	The amount and type of risk that Council is willing to accept or retain in pursuit of its objectives.
Risk Tolerance	The acceptable level of variation in performance outcomes that Council is willing to tolerate before corrective action is required.
Inherent Risk	The level of risk that exists before any controls or mitigation measures are applied.
Residual Risk	The level of risk remaining after controls or treatments have been implemented.
Likelihood	The chance or probability of a risk event occurring.
Consequence	The outcome or impact that would result if a risk were to materialise.
Risk Rating	A value or category assigned to a risk based on its assessed likelihood and consequence, used to determine its significance and priority.
Control	Any policy, procedure, practice, device, or action that modifies risk. Controls can reduce the likelihood of a risk occurring or the severity of its consequences.
Control Effectiveness	An assessment of how well a control is designed and operating to mitigate the risk it is intended to manage.
Risk Treatment	The process of selecting and implementing measures to address risks, including actions to avoid, reduce, transfer, or accept risk.
Risk Mitigation	Actions taken to reduce the likelihood or impact of a risk.
Risk Owner	The person or position accountable for managing a specific risk, including monitoring and implementing treatments.
Control Owner	The person or position responsible for implementing and maintaining a specific control.
Council	Muswellbrook Shire Council, the governing body responsible for strategic oversight, policy setting, and ensuring sound risk governance.
Risk Register	A centralised tool used to record identified risks, including their causes, impacts, risk ratings, controls, treatments, and responsible parties.
ERM Framework	The overarching document that defines the principles, approach, roles, processes, and tools used by Council to manage risk consistently.
Risk Categories	A structured classification of risks used by Council to ensure comprehensive risk identification across areas such as governance, finance, people, legal, environment, technology, and service delivery.

## 5. Policy Statements

Council recognises that the purpose of Risk Management is the creation and protection of value and is committed to managing risk to improve performance, encourage innovation and support the achievement of objectives. This understanding is reflected in the following Risk Management commitments adopted by Council:

- Risk Management practices encompass the entire organisation, creating connections to avoid silos.
- Risk Management Strategies address the full spectrum of risks and are appropriately scaled to reflect situational context and complexity.
- Risk Management approaches encompass risk scenarios and the interaction of multiple risks rather than considering single events.
- Risk Management practices are integrated into business culture and procedures to ensure that strategy and decision-making evolve from a risk informed process.
- Risk Management philosophy focuses on acceptable risk action rather than on risk avoidance.
- Council will make the necessary resources available to manage risks.
- Council is committed to managing risk within Council's Risk Appetite by identifying, analysing, evaluating and treating exposures that may impact on Council achieving its Objectives and/or the continued efficiency and effectiveness of its operations.
- Council will incorporate Risk Management into its planning and decision-making processes and subsequently into its business execution.
- Council will periodically review its Objectives and Appetite to achieve them to ensure that there are no conflicts, and where there are, address those conflicts as soon as practicable.
- Council's Risk Management process will be aligned to relevant standards and best practice in a manner that aligns with the organisation's culture and maturity.
- Council staff will implement and embed the Risk Management process into Council's business practices to reinforce their decision-making responsibilities and accountability.
- Council is committed to ensuring that all staff, particularly those with management, advisory, and decision-making responsibilities obtain a sound understanding of Risk Management Principles and the requisite skills to implement Risk Management effectively.
- Council will regularly monitor and review the status of its risk culture throughout the organisation as a basis for continuous improvement.
- Council is committed to continually improving its ability to manage risk.
- Council will review this Policy and its Enterprise Risk Management Framework at least annually.

## 6. Roles, Responsibilities and Delegations

To achieve its Strategic Objectives, Council must effectively manage the threats and opportunities associated with its operations, services, and decisions. A strong and consistent approach to Enterprise Risk Management enables Council to protect community value, build stakeholder confidence, and enhance the efficiency of its services.

In line with AS ISO 31000:2018, the Council and Audit, Risk and Improvement Committee (ARIC) are accountable for overseeing risk management, while the General Manager, Directors, and Managers are accountable for ensuring that risk management is integrated into all organisational activities and decision-making processes.

Risk Management must be championed by the General Manager, overseen by the Council and the ARIC, implemented by the Directorate and Management Leadership Groups, and actively applied by all staff, volunteers, and contractors. The Manager of Governance and Risk, supported by the Coordinator Enterprise Risk and Insurance, plays a central role in guiding, coordinating, and embedding the Enterprise Risk Management Framework across the organisation.

The specific roles and responsibilities for Risk Management are detailed in Council's Enterprise Risk Management Framework and supporting position descriptions.

## 7. Dispute Resolution

The General Manager is the interpreter of this Policy and shall be the sole arbiter in respect to the application of this policy.

## 8. Related Documents

### Legislation and Guidelines

- Local Government Act (NSW) 1993
- Local Government (General) Regulation 2005
- Guidelines for Risk Management and Internal Audit for Local Government in NSW, NSW Office of Local Government 2023
- AS ISO 31000:2018 Risk management – Guidelines
- ISO Guide 73:2009 Risk management – Vocabulary
- ISO 31010:2009 Risk management – Risk assessment techniques.

### Other Supporting Documents

- Enterprise Risk Management Framework
- Enterprise Risk Management Tools and Registers

## 9. Version History

This section identifies authors who reviewed the Policy and the date that it became effective.

V.	Date	Modified by	Amendments/Previous adoption details
1.	30/06/2020	Manager, Integrated Planning, Risk and Governance	First version. Adopted by Council 30 June 2020, minute number 402.
2.	08/08/2025	Manager Governance and Risk	Rewritten to ensure alignment with updated OLG Guidelines and the <i>Local Government (General) Regulation 2021</i> .

This document is a controlled document. Before using this document, check it is the latest version by referring to Council's EDRMS and ensuring you are using the Last Approved Version. Printed or downloaded versions of this document are uncontrolled.