CUMBERLAND
CITY COUNCIL

Risk Management Policy

AUTHORISATION & VERSION CONTROL

Policy Number	POL-049
Policy Owner	Director Governance and Risk
Date Adopted	19 June 2024
Version No	2
Document ID Number:	5893063
Review Date	June 2028

1. Purpose

The purpose of this Policy is to outline Cumberland City Council's (Council's) commitment to implementing organisation-wide risk management principles, systems and processes that support the consistent, efficient and effective assessment of risk in all Council's planning, decision-making and operational processes.

Under s8B(c) of the *Local Government Act 1993* (LG Act), Council should have effective financial and asset management, including sound policies and processes for risk management practices.

Risk management is an essential part of effective corporate governance and is a process by which the organisation can identify, analyse and manage risks.

While the General Manager (GM) is responsible for the design, implementation and operation of the organisation's risk management and internal control framework (RM Framework), it is essential that the elected Council (Governing Body) establish the foundational elements of Council's RM Framework, support good risk management, provide independent oversight, and approve, by resolution through this Policy, the risk appetite of the organisation.

2. Definitions

The definition of '*risk*' and '*risk management*' adopted by Council are reflective of the definitions provided in the current Australian Risk Management Standard (ISO 31000:2018), as follows:

- **Risk** means the effect of uncertainty on objectives, where an effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats.
- **Risk management** means coordinated activities to direct and control an organisation with regard to risk.

3. Scope

Council aims to create a positive risk management culture where risk management is integrated into daily activities, and managing risks becomes an integral part of governance, good management practice and decision-making.

All staff members and business units are responsible for observing and implementing this Policy, and Council's RM Framework.

Therefore, this Policy applies to all Council officials, as defined in Council's Code of Conduct (including Councillors, staff, contractors and volunteers) (Personnel).

4. Risk Management Framework

Council provides critical services and infrastructure to the residents, ratepayers and visitors within the Cumberland Local Government Area (LGA). Council also has service agreements and contractual obligations with government, non-government agencies, and private organisations, and has its own strategic goals and objectives that it seeks to achieve on behalf of the Cumberland community.

It is therefore incumbent on Council to understand the internal and external risks that may impact the delivery of those services, contracts and strategic objectives, and have processes in place to identify, mitigate, manage and monitor those risks to deliver the best outcomes for Council's personnel and the wider community. It is also Council's responsibility to maintain the efficient, effective and ethical use of resources and services by ratepayers, residents, personnel and visitors.

Council has developed a RM Framework consistent with ISO 31000:2018 to assist it to identify, manage, monitor and review all risks to its operations and strategic objectives, and to apply appropriate internal controls.

Council is committed to upholding the principles and methodologies published in ISO 31000:2018. This commitment extends to the complete integration of risk management within the organisational fabric, ensuring it is applied across all facets of Council's decision-making, operational and regulatory functions, services, and other activities. This dedication aligns seamlessly with Council's statutory obligations, reinforcing its unwavering commitment to sound risk management practices.

Risk management is integrated into Council's operations through the implementation and ongoing monitoring of the following:

- strategic risk register in alignment with Council's corporate plan;
- operational risk registers linked to the strategic risk register;
- project risk assessments with the development of project plans;
- risk matrix results, provided on a bi-annual basis to the ARIC;
- completion of fraud risk assessments;
- business continuity management plan and testing;
- procurement risk assessments as required under Council's Procurement Operational Procedure;
- insurance policy coverage as required under the LG Act;
- risk management advice and reporting in all Council and ARIC reports;
- robust risk training and review program; and
- robust Work Health and Safety (WH&S) system.

The RM Framework ensures that any risk-related information derived from these activities is adequately reported and used as a basis for decision-making and accountability across the organisation.

5. Key Principles

As required by ISO 31000:2018, Council's RM Framework must demonstrate the following six (6) elements:

Key Element	Requirement for Achievement
Leadership and Commitment	Risk management must be supported by a positive culture that promotes and communicates risk management as part of everyday activities and decision-making. This culture can only exist when management (including the Governing Body, GM and senior personnel) demonstrate strong leadership and commitment to risk management.
Integration	Risk management is fully integrated within Council and made part of its purpose, governance, leadership, strategy, objectives and operations. Risk must be managed in every part of Council's organisational structure and all Council personnel are responsible for managing risk.
Design	The design of Council's RM Framework: 1. is based on the unique needs, characteristics and risks of Council, and its external and internal context; 2. demonstrates Council's continual commitment to risk management; 3. assigns risk management roles, responsibilities and accountabilities within Council; 4. allocates appropriate resources for risk management; and 5. effectively documents and communicates risk management across the organisation.
Implementation	Council implements its RM Framework by: 1. developing a risk management plan that provides the structure implementation and management of Council's *Risk Management Policy*; and 2. ensuring Council's risk management activities are clearly understood and practiced. The RM Framework should identify decision makers for risk within Council and provide that risk management processes and arrangements are well understood by all personnel and practiced accordingly.
Evaluation	Council must regularly evaluate the effectiveness of its RM Framework and determine whether it remains relevant.
Improvement	Council continually adapts and improves the design and integration of its RM Framework to help Council move toward a higher level of risk maturity.

Internally, Council's RM Framework is also underpinned by these principles:

1. **Consistency:** promoting transparency and applying a consistent RM Framework across the organisation.

2. **Flexibility:** in approach in how we identify, respond and control risk to accommodate the various range of activities across Council.

3. **Accountability:** reinforcing risk accountability structures across all Council personnel.

4. **Embedded risk culture:** where possible, risk management will be embedded in our culture, strategies, plans, decisions, operations, recruitment and business processes.

5. **Review and monitoring:** undertaking regular monitoring, review and reporting of risks.

6. **Education and awareness:** driving a positive risk culture and awareness through education and training.

6. Assessment of Risk

6.1 Risk Hierarchy

There are different types of risks within Council. These are outlined in Figure 1 below and should be considered when considering risks generally:

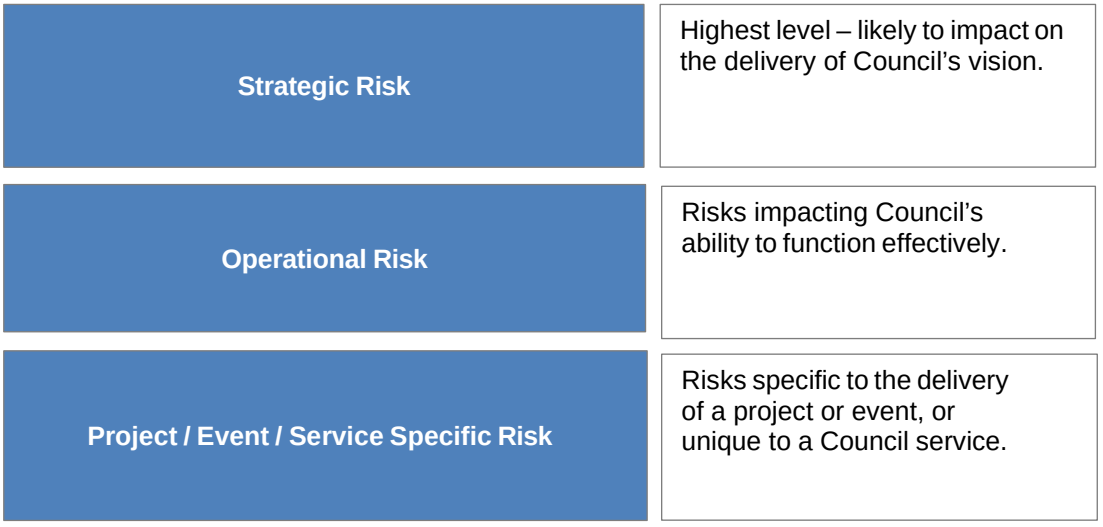
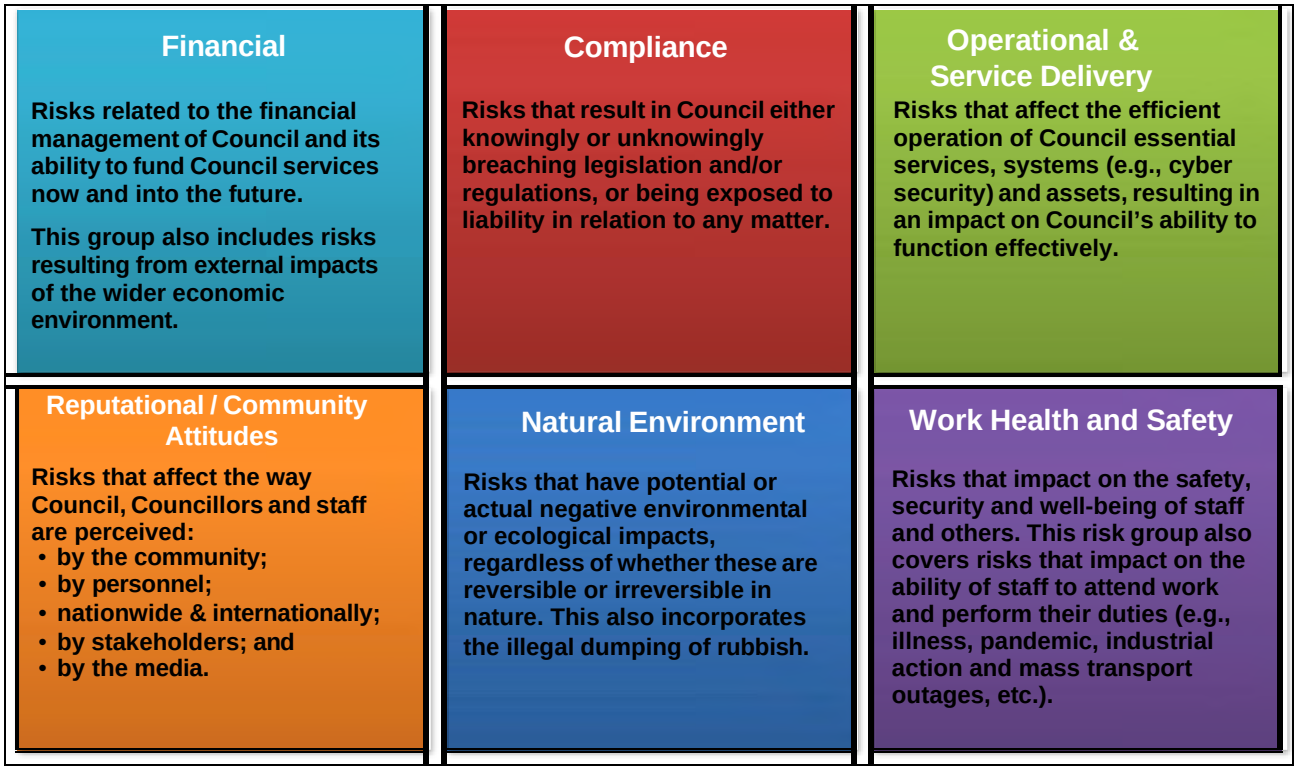


Figure 1: Risk Hierarchy Levels

6.2 Risk Categories

Risk events derive from, or impact in, one or more of the categories below.



When conducting risk analysis, Council personnel are required to identify all risks as belonging to one or more of these risk categories.

6.3 Risk Appetite Statements

Council's risk appetite statements express the general level of risk Council is willing to accept in order to meet its objectives and aspirations.

The Governing Body is responsible for determining the level of risk exposure that is considered acceptable.

Council's risk appetite is defined through the risk statements below and the risk tolerances articulated in the risk rating criteria. The risk tolerances are reviewed periodically by the Governing Body or delegated members.

Categories	Appetite Statement
Financial	1. Council has a **low** appetite for any financial decision resulting in a significant loss. The long-term financial plan ensures Council remains financially sustainable into the future as financial risks and rewards will be assessed against both our short and long term strategic and operational priorities. 2. Council has a **moderate** appetite for risk associated with the investment of Council's capital on interest earning funds.
Compliance	1. Council has a **low** appetite for compliance breaches. 2. Council has **no** appetite for internal fraud, corruption, collusion, bribery or theft. 3. Council has a **low** appetite for non-compliance with legal, professional and regulatory requirements.
Operational and Service Delivery	1. Council has a **moderate** appetite for technology risk and innovation. 2. Council has **no** appetite for negative impacts to essential services, for example, waste management.
Reputational/ Community Attitude	Council has a **low** appetite for risk associated with reputational/community attitude. Council is willing to take a low-risk approach, ensuring strong community engagement, transparency and increased participation within the community is achieved.
Natural Environment	Council has **no** appetite for illegal dumping of contaminated waste or destruction of endangered species, either localised or widespread, causing minor or irreversible damage to aquatic or terrestrial ecosystems.
Work Health and Safety	Council has **no** appetite for practices or behaviours that could lead to any personnel being harmed physically or psychologically while at work. Council is committed to creating a safe working environment, fostering a culture that values continuous learning and collaboration. This unwavering dedication to the welfare of personnel reflects the Council's steadfast commitment to fostering a workplace where safety, well-being, and professional growth are prioritised.

7. Risk Management Process

A risk management process is a systematic way of establishing the context in which the whole of Council operates by identifying, analysing, evaluating and treating the risks which may provide uncertainty around its ability to achieve its objectives.

A risk management process also provides a structure to ensure that identified risks are continuously monitored and reviewed. The diagram in Figure 2 describes the standard process for risk management, as set out in ISO 31000:2018.

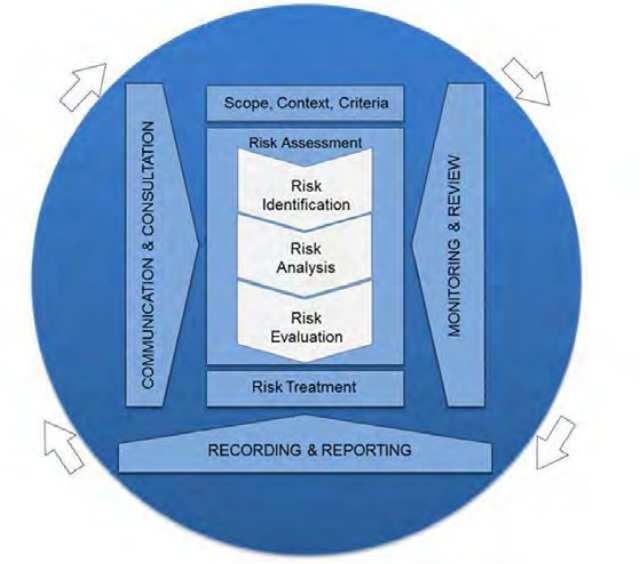


Figure 2 – Standard Process for Risk Management – ISO31000:2018

Communication and consultation are ongoing activities across all stages of the risk management process to provide, share, engage and obtain information from internal and external stakeholders regarding the management of risk.

7.1 Roles and Responsibilities

Council aims to create a positive risk management culture where risk management is integrated into all daily activities across the organisation, and managing risks becomes an integral part of governance, good management practice and decision-making.

All Council personnel have a responsibility to observe and implement this Policy and Council's RM Framework.

The success of Council's RM Framework requires the full support of all stakeholders, including the Governing Body and the Executive Team, to deliver a fully embedded RM Framework and positive internal risk culture. This is an integral part of ISO 31000:2018, as outlined below.

Figure 3 – Leadership Commitment to Risk Management - ISO31000:2018

The following table identifies the roles and responsibilities of all stakeholders in Council's RM Framework:

Role	Responsibilities
Governing Body	The Governing Body (i.e., elected Council) is responsible for setting the risk appetite statements for the organisation. The Governing Body is also required to consider all available information provided to them by management and make decisions for the wider community having regard to public interest and any associated risk.
Chief Risk Officer	The Director of Governance and Risk will act as Council's Chief Risk Officer and has primary accountability for risk management activities on behalf of Council. The Chief Risk Officer will ensure that a risk management system is established, implemented, monitored, and maintained with appropriate resourcing allocated in accordance with this Policy and the RM Framework.
General Manager	The GM must promote a positive risk culture within Council and keep the Governing Body properly informed of any risks. The GM is also responsible for endorsing any strategic risks and implementing Council's risk appetite and tolerance levels in accepting certain risks.
Manager of Audit, Safety and Risk	The Manager of Audit, Safety and Risk will oversee risk management across Council, taking advice from the ARIC and the Executive Team. More specifically they will: • assess and recommend amendments to this Policy and the RM Framework. • monitor key risks on the risk register and where applicable, recommend appropriate actions or improvements affecting Council's risk register/exposure.

	• provide timely and adequate information to the ARIC and Executive Team on the status of Council's key risks. • develop an organisation-wide risk training plan. • provide reports to the ARIC and Executive Team on the status of risk management implementation and effectiveness across Council. • in conjunction with the Human Resources team, implement the organisation-wide risk training plan. • be a point of contact for personnel with questions on risk management.
Coordinator Audit and Risk	The Coordinator of Audit and Risk is the point of contact for advice on the implementation and administration of this Policy and the RM Framework. The Coordinator of Audit and Risk has responsibility to deliver the following outcomes: • that appropriate risk management processes are supported and administered throughout Council. • Council-wide risk registers are updated following the review of key risks. • consider the RM Framework in planning and conducting audits. • review the control environment and insurance arrangements. • report on key audit findings to the ARIC. • act as a knowledge base and be a point of contact for personnel with questions about risk management. • provide feedback on risk and insurance related issues and participate in periodic advisory panels.
ARIC	In overseeing that Council is effectively managing its risk and complying with its statutory obligations, Council's ARIC is responsible for monitoring that Council has the following in place: • risk management processes and procedures; • risk management strategies for major projects or undertakings; • business continuity planning arrangements; • a fraud control plan; and • a sound internal control environment.

Executive and Senior Leadership Team	Risk management is a core responsibility for all Senior Management at Council. In addition to their broader responsibilities, Council's Executive and Senior Leadership teams are responsible for the following: • ensure that all personnel effectively monitor and manage the risks within their own work areas. Risks should be anticipated, and reasonable protective measures taken. • encourage openness and honesty in the reporting and escalation of risks. • ensure all personnel have the appropriate capability to perform their risk management roles. • identify and communicate any improvement opportunities in Council's risk management practices and RM Framework to the Chief Risk Officer.
Managers and Supervisors	Managers and Supervisors are responsible for overseeing the operation and the management of risks within their areas of responsibility. They are required to: • own all risks within their area of responsibility. • ensure appropriate processes are in place within their areas to ensure that all risks impacting on achieving objectives or realising opportunities are identified, assessed, managed, and reviewed on a regular basis within agreed tolerance levels. • be a champion for risk management within their area. • review and update relevant risk registers. • ensure the cost-effective management of risk. • inform the relevant Executive Manager or Director of significant changes to key risks which impact upon the Council. • always consider risk as a part of their decision-making processes.
Project Managers and Contractors	Project managers and contractors are expected to understand the RM Framework in the context of project management, adopt a risk-based approach in their management, and lead by example in their behaviour in the workplace, ensuring that risk assessments and risk registers are established for all key risks in their area of responsibility.
All Personnel	All Council personnel are responsible for identifying and managing risk within their work areas. All personnel are required to: • be familiar with, and understanding of, the principles of risk management. • comply with all policies, procedures and practices relating to risk management. • alert Executive and/or Senior Management to risks that exist within their area. • perform any risk management activities assigned to them as part of their daily role.

8. Monitoring, Review and Escalation

8.1 Monitoring and Review

Council is committed to continually improving its ability to manage risk. Council Officers will review this Policy and its RM Framework regularly to ensure Council's RM Framework is in adherence with the requirements of the *Local Government Act 1993*, the *Local Government (General) Regulation 2021* (Regulation), and Council's requirements, as well as ISO 31000:2018 RM Standard.

The GM will be required under the Regulation to attest each year in Council's annual report whether Council has complied with the requirements prescribed under the Regulation in relation to its risk management activities. The ARIC will oversee Council's RM Framework. In addition:

- The Governing Body will be engaged at a strategic level and will receive periodic reports from management through the ARIC on material risks (where risks are rated 'major' or 'catastrophic').
- The Executive Team will receive updates of any changes to the strategic risk profile, engaged at a strategic level and will contribute to the annual organisation-wide strategic risk register.
- The Executive Team will participate in the identification, assessment and rating of operational risks through the operational risk review process.
- Councils RM Framework will be subject to Internal Audit and be listed on the Internal Audit Strategic 4 year Work Plan.

8.2 Escalation Process

The risk escalation process is outlined below:

Residual Rating	Escalation Process
Catastrophic	• Immediate attention of GM. • ARIC Chairperson to be informed. • Governing Body to be informed.
Major	• Immediate attention of the Executive Team. • Updates provided in the monthly Executive meeting. • Report provided on a quarterly basis to the ARIC. • Treatments prepared by risk owner for Executive Management approval.
Moderate	• Immediate attention of Manager. • Treatments prepared by risk owner for Manager approval. • Executive Management to be informed in team meeting.
Minor	Risk to be managed through routine 'business as usual' process to support ongoing monitoring in case the risk profile changes.
Insignificant	Risk descriptor does not impact the business unit and does not require any ongoing monitoring.

9. Related Documents and Council Policy

- Risk Management Guidelines
- Fraud and Corruption Control Policy
- *Local Government Act 1993*
- *Work, Health and Safety Act 2011*
- (AS/NZS) ISO 31000:2018 – Risk Management
- AS/NZA ISO 45001:2018
- *Civil Liability Act 2002*
- Work Health and Safety Management System

Review Page

Reviewed by:

Chairperson of ARIC	**General Manager, in accordance with Council Resolution** _____
Signature	Signature
Name	Name
Date	Date