CUMBERLAND
CITY COUNCIL

Risk Management Policy

AUTHORISATION & VERSION CONTROL

Policy Number	POL-049
Policy Owner	General Manager's Unit
Date Adopted	18 December 2019
Version No	1
Document ID Number:	5893063
Review Date	December 2021

PURPOSE

Under the *Local Government Act 1993* Sect 8B (c), Council must apply effective financial and asset management including sound policies and process 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 treat risks. While the General Manager is responsible for the design and operation of risk management and the internal control framework, it is essential that the elected Council support good risk management, provide independent oversight, and set the risk appetite of the organisation.

This Policy aims to drive risk informed decision making, ensuring that Councils operations and activities are aligned with Council's Risk Appetite statements. This policy clearly communicates Councils commitment to maintaining an effective and efficient risk management framework.

SCOPE

This policy applies to all Cumberland City Council Officials as defined in the Code of Conduct. This includes all Councillors, Council staff, Contractors and Volunteers.

RISK MANAGEMENT FRAMEWORK

Councils Risk Management practices are based on the International Standard for Risk Management (ISO31000:2018) which describes risk management framework as a set of components that provide the organisation to self-identify, develop and implement strategies to improve their risk management maturity.

Risk management is integrated into Councils operations through the undertaking of:

- A strategic risk register in alignment with Councils Corporate Plan
- An operational risk register linked to the Strategic risk register
- Project risk assessments with the development of project plans
- Risk matrix results, provided on a quarterly basis to the Audit and Risk Committee (ARIC)
- Completion of Fraud risk assessments;
- Business continuity management plan and testing
- Procurement risk assessments as required under Cumberland City Council's Procurement Operational Procedure;
- Insurance policy coverage as required under the *Local Government Act 1993.*
- Risk Management advice and reporting in all Council and Audit, Risk and Improvement Committee reports.

The risk management framework ensures that risk information derived from these activities is adequately reported and used as a basis for decision-making and accountability across all relevant levels.

PRINCIPLES

This ERM framework is underpinned by the following principles:

- **Consistency:** Promoting transparency and applying a consistent Risk framework across the organisation.
- **Flexibility:** in approach in how we identify, respond and control risk to accommodate the various range of activities across Council.
- **Accountability:** Reinforcing risk accountability structures in all levels of staff.
- **Embedded risk culture:** risk management where possible will be embedded in our culture, strategies, plans, decisions, operations, recruitment and business processes.
- **Review and monitoring:** Undertaking regular monitoring, review and reporting of risks.
- **Education and awareness:** Driving a positive risk culture and awareness through education and training.

DEFINITIONS

- **Risk -** Defined in the ISO 31000:2018 standard as the "Effect of uncertainty on objectives – a deviation from the expected – positive and/or negative and can address, create of result in opportunities or threats".

Each of the terms are further defined below:

- **Effect:** Deviation from the expected – positive or negative.
- **Objectives:** Can have different aspects and can apply at different levels
- **Risks:** Often characterised by reference to potential events and consequences, and is often expressed in terms of a combination of consequences of an event and the associated likelihood
- **Uncertainty:** The state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequence, or likelihood.

Risk Hierarchy

There are different types of risks within Council. The different risk types are outlined in figure 1 below and should be considered when considering risks:

Figure 1: Risk Hierarchy Levels

RISK CATEGORIES

Risk events derive from, or impact in, one or more of the below categories. When conducting risk analysis, Council staff are required to identify all risks as belonging to one or more of these risk categories:

Financial

Risks related to the financial management of Council and its ability to fund Council services now and into the future.

This group also includes risks resulting from external impacts of the wider economic environment.

Compliance

Risks that result in Council either knowingly or unknowingly breaching legislation and/or regulations, or being exposed to liability in relation to any matter.

Operational / Service Delivery

Risks that affect the efficient operation of Council services, systems (e.g. cyber security) and assets, resulting in an impact on Council's ability to function effectively.

Reputational / Community Attitudes

Risks that affect the way Council, Councillors and staff are perceived:

By the community
By staff
Nationwide & internationally
By stakeholders
By the media

Natural Environment

Risks that have potential or actual negative environmental or ecological impacts, regardless of whether these are reversible or irreversible in nature. This also incorporates the illegal dumping of rubbish.

Human Resources

Risks that impact on the safety, security and well-being of staff and others. This risk group also covers risks that impact on the ability of staff to attend work and perform their duties (e.g. illness, pandemic, industrial action and mass transport outages, etc.).

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. Councillors are 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 which are reviewed periodically by the Councillors and delegated members.

Categories	Appetite Statement
Financial	• Council has a **low appetite** for any financial decision resulting in a significant loss. The long term financial plan ensures Cumberland City 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 • Council has a **moderate appetite** for risk associated with the investment of Council's capital on interest earning funds.
Compliance	• Council has a **low appetite** for compliance breaches. • Council has **no appetite** for internal fraud, corruption, collusion, bribery or theft. • Council has a **low appetite** for non-compliance with legal, professional and regulatory requirements.
Operational/ Service Delivery	• Council has a **moderate appetite** for technology risk and innovation. • Council has **no appetite** for negative impacts to core services e.g. waste
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, either localised or widespread, causing minor or irreversible damage to aquatic or terrestrial ecosystems.
Human Resources	• Council has **no appetite** for practices or behaviours that could lead a staff member 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.

RISK MANAGEMENT PROCESS

A risk management process is a systematic way of establishing the context in which the Council, business unit or project 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.

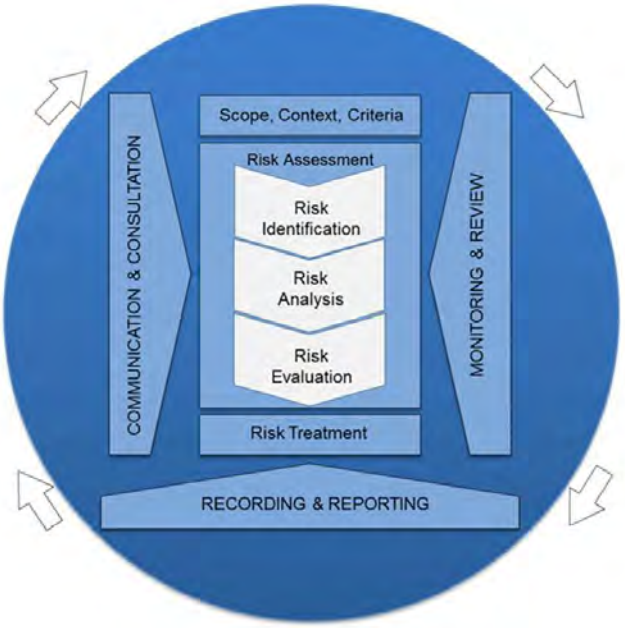

Figure 2 – Standard Process for Risk Management – ISO31000:2018

Communication and consultation is a continual activity 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.

ROLES AND RESPONSIBILITIES

The success of Council's risk management framework requires the full support of all stakeholders, including the Council, Executive and Leadership team in order to deliver a fully embedded risk framework and positive staff risk culture. This is an integral part of the ISO:31000 Risk Management Framework, as outlined below.

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

The following table identifies the roles and responsibilities of all stakeholders in the Enterprise Risk Management Framework:

Role	Responsibilities
Elected Council	The elected Council is responsible for setting the Risk Appetite Statements for the organisation. Council is also required to consider all available information provided to them by Management and make decisions for the greater community in the public interest, with consideration to the Risk Appetite statements set. Therefore, the Council has the ultimate responsibility for ensuring that Risk is appropriately managed across Council.
Chief Risk Officer	The Executive Manager General Manager's Unit will act as Council's Chief Risk Officer and has primary accountability for risk management activities on behalf of Council. They will ensure that a risk management system is established, implemented and maintained in accordance with the Policy and these Guidelines.
General Manager	Will promote a positive risk culture within Council and keep elected officials properly informed of relevant risks in all Council reports. Responsible for endorsing strategic risks and implementing Council's risk appetite and tolerance levels in accepting certain risks.
Executive Manager General Manager's Unit	Will oversee risk management across Council, taking advice from the Audit, Risk and Improvement Committee (ARIC) and Council's Leadership Team. More specifically they will: • Assess and recommend amendments to the *Risk Management Guidelines*. • Monitor key risks on the risk register and where applicable recommend appropriate actions/improvements affecting Council's risk register/exposure. • Provide timely and adequate information to the Leadership Team and the ARIC on the status of Council's key risks. • Development of an organisation wide Governance and Risk Training Plan. • Ensure reports are provided to the ARIC and the Leadership Team on the status of risk management implementation and effectiveness across Council.
Audit & Risk Management Coordinator	Primary point of contact for advice on the implementation and administration of these Guidelines. Key administrator of the Enterprise Risk Management Framework, who will undertake the role of 'in house' risk practitioner. The Risk Management Coordinator has responsibility to ensure: • Appropriate risk management processes are supported and administered throughout Council. The Council wide risk registers are updated following the review of key risks. • Necessary risk reporting and supporting documentation is prepared. • Act as a knowledge base and be a point of contact for staff with questions on risk management. • Provide feedback on risk and insurance related issues and participate in periodic advisory panels. • Implementation, in conjunction with the Human Resources Team, of the organisation wide Governance and Risk Training Plan.
Audit, Risk and Improvement Committee	Provides general oversight and monitoring of the effectiveness of the Enterprise Risk Management framework. Specifically the Committee will: • Ensure that Council audit plan and scopes for individual audits are adequate to give assurance that risks are well managed. • Advise Council annually, via the ARIC Chairman's report to Council, on the effectiveness of risk management activities.
Internal Audit	• Consider the risk management framework in planning and conducting audits. • Provide advice and assurance over Council's risk management framework. • Also reports on key audit findings to the Audit, Risk and Improvement Committee.
Leadership Team	• Responsible for overseeing the operation of these Guidelines and the management of risks within their areas of responsibility. The Leadership Team is required to: • Ensure risk management is embedded into the key controls and approval processes of all major business processes, projects and functions within their respective areas of responsibility. • Own all risks within their respective area of responsibility and be responsible for ensuring managers collectively fulfil their risk management responsibilities in their respective areas. • Ensure risk registers are maintained and current for their operational groups. • Evaluate and ensure prioritised and effective action is taken to mitigate the key risks faced by Council, and ensure that this prioritisation process and resulting actions are incorporated into Council's annual planning and budget processes.

Managers and Supervisors	Responsible for overseeing the operation of these Guidelines and the management of risks within their areas of responsibility. Managers 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. • Update relevant risk registers. • Ensure the cost-effective management of risk. • Inform their Executive Manager of significant changes to key risks which impact upon the Council. Consider risk as a part of their decision-making processes.
Project Managers and Contractors	Project managers and contractors are expected to understand the risk management framework, 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 Staff	Employees and contractors will perform their duties and functions in a safe manner, adhering to the *Code of Conduct*, safe work practices and ensuring that they are familiar with the Council's Risk Management Framework. All individuals will play a part in managing risk at Council, by identifying risks in their area and contributing to the implementation of risk treatments.

MONITORING, REVIEW AND ESCALATION

- The Audit, Risk and Improvement Committee will oversee Council's risk management framework.
- Elected Council will be engaged at a strategic level and will receive periodic reports on material risks (where risks are rated 'major or catastrophic').
- The Executive and Leadership teams 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 also participate in the identification, assessment and rating of operational risks through the six monthly operational risk review process.
- Councils Risk Management Framework will also be subject to Internal Audit, and will be listed on the Internal Audit Program.
- The residual risk escalation process is outlined below:

Residual Rating	Escalation Process
Catastrophic	• Immediate attention of General Manager • Tabled at Councillor meeting with treatments prepared by Risk Owner for considerations • Councillors to be informed as appropriate
Major	• Immediate attention of Executive Management Team • Updates provided in the monthly Executive Management 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 Member 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

RELATED DOCUMENTS AND COUNCIL POLICY

- Risk Management Guidelines
- (AS/NZS) ISO 31000:2018 – Risk Management
- Procurement Operational Procedure
- Local Government Act 1993
- Work, Health and Safety Act 2011
- Civil Liability Act 2002