NORFOLK ISLAND
Regional Council

2.13.00 – RISK MANAGEMENT FRAMEWORK

1 PURPOSE

The purpose of this Framework is to ensure that Council implements a structured approach for identifying, assessing, and managing risks across Council. The Risk Management Framework helps to ensure that risks are proactively identified and effectively managed to protect Council's operations, reputation, and ongoing financial sustainability. It also fosters collaboration and communication among stakeholders to ensure that risks are managed consistently throughout Council.

2 OBJECTIVE

The objective of the Risk Management Framework is to enable Council to effectively achieve its goals by reducing the likelihood and impact of risks while maximising opportunities for success. This is achieved by developing and implementing effective risk management policies and processes that identify, assess, treat, and monitor risks in a structured and informed manner. The Risk Management Framework will be flexible and be adaptable to changing circumstances, enabling Council to respond quickly to new or emerging risks. Ultimately, the Risk Management Framework aims to promote a culture of risk awareness and accountability, ensuring that risks are managed systematically and consistently throughout the Council.

3 SCOPE

This Framework applies to all elected representatives, officers, employees, contractors, committee members and volunteers of Council; and to all Council activities, including any entities where Council has direct ownership, management, sponsorship or financial control.

This Framework applies to all functions, processes, and activities within Council, including but not limited to strategic planning, financial management, human resources, health and safety, and environmental management.

4 DEFINITIONS

TERM	DEFINITION
Council	Norfolk Island Regional Council
Community	Norfolk Island Regional Council residents, ratepayers and other users of Council's services and assets, as well as key agencies and stakeholders holding a vested interest
Levels of Risk	Risks are categorised based on the likelihood and potential impact of an adverse event as follows: • "Low risk" - A risk that is unlikely to have a significant impact on objectives or operations or one that can be easily managed with existing controls. • "Moderate risk" - A risk that could have a noticeable impact on objectives or operations and may require additional controls or management.

	• "High risk" - A risk that is likely to have a significant impact on objectives or operations and may require significant resources or management attention to address. • "Extreme risk" - A risk that could result in a severe or catastrophic impact on objectives or operations and may require immediate and significant action to address.
General Manager	A person who holds an appointment under section 334 of the *Local Government Act 1993* (NSW) (NI). This includes a person acting in this position.
Risk	A risk to Council is any action or event that has the potential to impact the achievement of business objectives. Risk also arises as much from the possibility that opportunities will not be realised as it does from the possibility that threats will materialise or that errors will be made.
Risk Assessment	A process of identifying the cause and source of a risk, its positive and negative consequences, and the likelihood that those consequences can occur. The level of risk is determined through this process; refer to Risk Management Procedure for more detail.
Risk Management Framework	A set of components that provide the foundation and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.
Risk Management Policy	A statement of overall intent and the direction of an organisation related to risk management.
Risk Management Procedure	The systematic application of management policies, process and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk.
Risk Owner	A Council employee (usually a Manager/Team Leader level) authorised by the General Manager to manage a particular risk and is accountable for doing so.
Risk Types	Risk types refer to the various categories or classifications of risks that the Council faces.

5 LEGAL AND POLICY FRAMEWORK

Legislation, Policies and Documents:

Legislation*:*

- *Local Government Act 1993* (NSW) (NI).
  - *Section 8B(c) Principles of Sound Financial Management* - Councils should have effective financial and asset management, including sound policies and processes for: (iv) risk management practices.
  - *Section 8C (h) Integrated planning and reporting principles that apply to Councils* - The following principles for strategic planning apply to the development of the integrated planning and reporting framework by councils— Councils should manage risks to the local community or area or to the council effectively and proactively.
- *Norfolk Island Act 1979* (CTH).
- *Employment Act 1988* (NI).
- *Law of Negligence and Limitation of Liability Act 2008* (NI).
- *Fair Work Act 2009* (CTH).
- *Workplace Health and Safety Act 2011* (CTH).
- *Safety Rehabilitation and Compensation Act 1988* (CTH).

- *Freedom of Information Act 1982* (CTH).

Policies:

- Risk Management Framework.
- Risk Management Procedure.
- Work, Health and Safety Policy.
- Procurement Policy.
- Fraud and Corruption Prevention Policy.
- Norfolk Island Regional Council - Code of Conduct.
- Procedures for the Administration of the Model Code of Conduct

Documents:

- Australian Standard AS/NZS ISO 31000:2018.
- Audit Risk and Improvement Committee Charter.

6 IMPLEMENTATION

Communication

This policy is to be communicated to all staff and the community via the Council's website.

7 FRAMEWORK STATEMENT

Council recognises the inherent risks in its business activities, programs, services, projects, processes, and decisions. As defined in AS/NZS ISO 31000:2018 - Risk Management - Guidelines, risk management is a comprehensive approach that encompasses strategy, processes, culture, technology, standards, and knowledge to identify, analyse, evaluate, manage, treat, monitor, review, and communicate uncertainties encountered by Council. To achieve efficient and effective risk management Council is committed to implementing a structured and coordinated Risk Management approach that aligns strategy, processes, people, technology, and knowledge to manage risk.

The Risk Management Framework removes traditional divisions and includes thinking about risk, not just as involving a loss but as an occurrence that may provide opportunities with both positive and negative consequences. Council's responsibility and that of its employees, contractors, volunteers, and suppliers to manage risk are emphasised.

Implementing this Risk Management Framework will establish a structured process for identifying, analysing, evaluating, managing, treating, monitoring, reviewing, and communicating risks, ensuring a consistent and best-practice approach throughout Council. It will also encourage the integration of risk management into Council's overall governance, planning, management, reporting processes, policies, operations, values, and culture.

7.1 RISK MANAGEMENT FRAMEWORK INTEGRATION WITH COUNCIL'S COMMUNITY STRATEGIC PLAN

Integrating the Risk Management Framework with Council's mission and values ensures that risk management is aligned with Council's purpose and goals.

7.1.1 Council's Mission

The Norfolk Island Regional Council will provide local civic leadership and governance through good decision making, accountability and transparency. We will protect and enhance our unique culture, heritage, traditions and environment for the Norfolk Island People. We will do this through promoting

a healthy and sustainable lifestyle, by looking after our community assets, and by fostering a prosperous economy.
(Source: Norfolk Island Community Strategic Plan 2016 – 2026)

7.1.2 Council's Values

The Council embraces the following values (I CARE):

- Integrity
- Communication
- Accountability
- Respect
- Excellence

7.1.3 Integration

The Risk Management Framework is an essential tool for Council in achieving its Community Strategic Plan and operational objectives. By integrating risk management into its strategic and operational planning process, Council can better understand the risks associated with achieving its goals and develop strategies to manage and mitigate those risks.

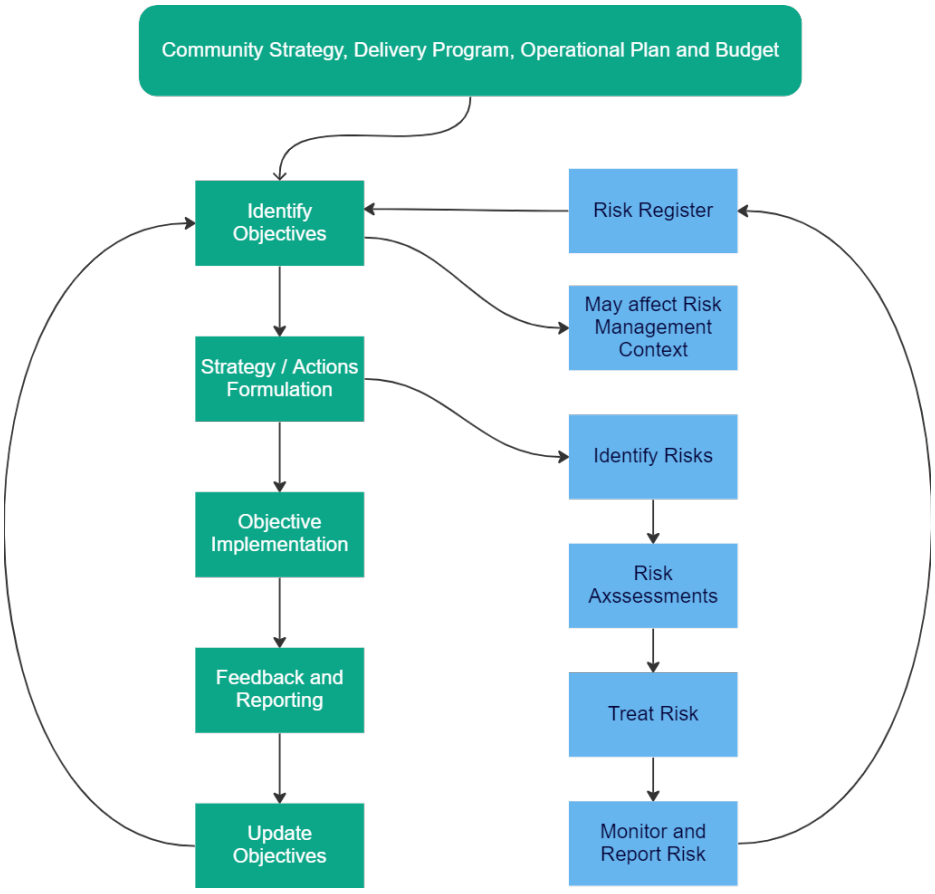

Figure 1 - Linking Strategic Planning with Risk Management

The Risk Management Framework will assist Council in identifying risks associated with its Community Strategic Plan activities and Operational Plan key targets and performance indicators, which will enable effective decision-making in support of the achievement of strategic and operational objectives.

Including identified risks under action or to be actioned in the delivery program and annual operational plan is essential for several reasons.

- It ensures that the risks are actively monitored and managed on an ongoing basis. By incorporating the identified risks into the operational plan, Council can prioritise risks, allocate resources and assign responsibilities to manage and mitigate them effectively.

- It enhances transparency and accountability in risk management. By including identified risks in the operational plan, Council can communicate to stakeholders, including the community, the risks it faces and the strategies it has to manage them.

- It supports the integration of risk management into Council's overall governance, planning, management, and reporting processes. By including risk management in the annual operational plan, Council can ensure that risk management is a fundamental part of Council's ongoing activities and not just an isolated or occasional task.

In summary, including identified risks in the delivery program and annual operational plan and budget is a critical step in the ongoing management and mitigation of risks, promoting transparency and accountability in risk management and integrating risk management into Council's overall processes.

7.2 COUNCIL'S RISK MANAGEMENT STANDARD

The following standards have been established to support Risk Management and provide clear guidance to risk owners on the approach required by Council:

Standard 1 - Support Audit Recommendations
This standard requires that risks identified through an internal or external audit be placed in the appropriate risk register, with the documented risk and any risk treatment plan being the responsibility of the risk owner.

Standard 2 – Learning from Incidents, Successes and Failures
This standard emphasises the importance of learning from incidents, successes, and failures to adjust the risk register accordingly and update the register in accordance with the *Risk Management Procedure*.

Standard 3 - Risk Ownership and Management
The risk owner is expected to maintain ownership and management of different of risk categories and risk types.

Risks identified through either an internal or external audit shall be placed in the appropriate risk register. A risk owner is a Council employee authorised to manage a particular risk and is accountable for doing so. The person is responsible for the following:

- ensuring that risks are identified, analysed, evaluated, treated, monitored, reviewed, and communicated promptly;
- developing and maintaining risk treatment plans that are consistent with the Council's risk appetite and objectives; and
- reporting on risks and the effectiveness of risk treatments to the Governance section and Council.

Risk owners are critical to the success of the *Risk Management Framework* as they are responsible for the day-to-day management of risks and ensuring that appropriate controls are in place to manage those risks.

To ensure effective risk management, management must maintain ownership of risks at a divisional and sectional level. However, they may allocate the day-to-day management of some lower-rated risks to Coordinators or Supervisors as needed.

Management are expected to maintain the overall ownership for risks relating to capital projects and major events unless the General Manager assigns risk ownership to another Council employee for a specific project or event. In any case, the risk owner is responsible for documenting the relevant risks in the risk register for reporting purposes.

7.3 COUNCIL'S ROLES AND RESPONSIBILITIES

Council's roles and responsibilities are clearly defined and outlined in the *Risk Management Policy*. Furthermore, the policy also differentiates the responsibility for managing risks within Council for the risk level at which it is assessed.

7.4 RISK CATEGORIES

Council has 3 main risk categories as follows:

Strategic Risk – Strategic risk refers to the potential negative impact on an organisation's goals and objectives from making incorrect or ineffective decisions regarding the allocation of its resources. It includes risks associated with the choice of strategy, its implementation, and the execution of plans. It can arise from various internal and external factors, including shifts in community preferences.

Operational Risk – Operational risk refers to the possibility of incurring losses or degradation of service quality due to unfavourable changes in conditions, processes, or other factors that could negatively impact the government's operations.

Project Risk - Project risk for a Council refers to the potential uncertainties and events that could affect the successful completion of a project, such as budget overruns, delays, or unexpected challenges.

7.5 RISK MANAGEMENT RESOURCES

Council should use its available resources efficiently and effectively to manage risk, minimising loss to the community and its assets. Insurance may be used to transfer or manage the risk of financial loss. However, in some instances, it may not be cost beneficial to do so and may not be transferable in every instance.

When considering the use of insurance, the following should be considered:

- Nature of the risk;
- Availability of alternative risk management and mitigation strategies;
- Cost of alternative risk management strategies;
- Financial consequences of choosing not to insure; and
- Level of loss Council is willing to fund.

Responsible officers must ensure they have the appropriate insurance for their specific risks. The level of insurance required should be based on tolerance levels, past claims experience, and the availability and cost of insurance. Officers should:

- Ensure they consider all insurable risks and insure appropriately; and
- Consider Council's risk profile and determine the appropriate level of insurance required.

Preventative and mitigating measures should be considered to reduce the probability or severity of an adverse risk event occurring if proven to be of cost-benefit, even if the risk has been insured. Regardless of whether the risk is able to be insured or not, the risk owner should document how the risk is to be managed via the risk register.

7.6 RISK APPETITE

Council's risk appetite is clearly defined and outlined in the *Risk Management Policy*.

As Low as Reasonably Practicable (ALARP). The Council will use the ALARP principle to ensure that resources are used appropriately and cost-effectively to reduce risk to acceptable levels. Council will consider ALARP to inform decisions about the trade-off between the cost of risk reduction measures and the potential benefits of improved safety or reduced liability.

7.7 RISK APPETITE & TOLERANCE PER TYPE

Understanding risk sources is crucial because it helps risk managers of Council identify and assess potential risks that could impact their operations or goals. By categorising risks, it becomes easier to prioritise them and allocate resources to mitigate or manage them effectively. Furthermore, understanding Council's appetite for each risk type can provide insight into the overall risk management strategy.

This knowledge can help individuals understand how Council approaches risk, how much risk it is willing to take, and what measures it has in place to manage risks within specific categories. Ultimately, this information can assist individuals in making informed decisions about their risk management strategies and align their practices with those of Council. Council encourages employees to consider all relevant policies and procedures, so that risk tolerance levels can be effectively managed and lowered where required.

RISK TYPE: HEALTH & SAFETY	
Risk Appetite Statement	**Risk Tolerance Statement**
Council has a **LOW RISK** appetite for risks that compromise the safety and welfare of staff, contractors, and/or members of the community. Council understands that some operations and services contain inherent risks. However, there is no appetite for compromising safety, particularly in the event of a serious injury or fatality, or for any deviations from the WH&S Policy and System Management Plan, Disaster Management Plan, and statutory WH&S provisions.	Council will **NOT** tolerate: • Actions or behaviours that are deliberate and willingly contravene the Councillor or Employee Codes of Conduct or WHS policies and procedures; • Activities that result in reasonably foreseeable and preventable injuries or illnesses to our community or employees; • Unsafe work environments; or • Risks that result in serious harm or loss of life.
Council Encourages	
Reporting and rectifying risks relating to safety and non-compliance in line with Councils WH&S Policy and System Management Plan, Disaster Management Plan, and statutory WH&S provisions.	

RISK TYPE: LEGAL AND COMPLIANCE	
Risk Appetite Statement	**Risk Tolerance Statement**
Council has a **LOW TO MODERATE RISK** appetite for risks related to compliance and legal requirements, with a focus on preventing significant breaches and legal claims.	Council will **NOT** tolerate: • Risks that result in significant financial penalties or legal action against Council; • Corrupt or fraudulent conduct by employees;

Council has no appetite for engaging in illegal activities, including fraud and corruption.	• Unreasonable delays when reporting, investigating, or correcting any fraudulent, improper, unethical or corrupt conduct; • Employees and Councillors knowingly breaking the law, failing to comply with legal obligations or recklessly breaching internal policies; • Employees and Councillors knowingly not complying with Council's policies and procedures; or • The unauthorised release of confidential information or privacy breaches.
Council Encourages	
An organisational culture that fosters compliance and immediate reporting to the Governance Section of potential or actual claims, cases, allegations or incidents.	

RISK TYPE: ENVIRONMENT	
Risk Appetite Statement	**Risk Tolerance Statement**
Council has a **LOW TO MODERATE RISK** appetite for risks related to environmental impact, with a focus on preventing significant and irreparable damage. Council will apply the precautionary approach to environmental decision making where there is uncertainty to avoid or minimise harm.	Council will **NOT** tolerate: • Risks that result in serious harm to the environment or that violate regulatory requirements.
Council Encourages	
Business activities and decisions that will aid in the long-term environmental sustainability of Norfolk Island.	

RISK TYPE: INFORMATION TECHNOLOGY (CYBER SECURITY)	
Risk Appetite Statement	**Risk Tolerance Statement**
Council has a **LOW RISK** appetite for risks related to Council's information technology environment including cyber security, with a particular focus on preventing significant breaches of sensitive data and system breaches. Council's focus is on appropriate internal controls to reduce the likelihood and consequences.	Council will **NOT** tolerate: • Council is intolerant of risks that result in serious harm to the Council's data or systems or that violate regulatory requirements; • Lack of preparation or planning in response to a cyber-attack; or • Misuse, inappropriate distribution, or loss of sensitive or confidential Council information due to employees' actions.
Council Encourages	
Employees to play their part and apply technical and behavioural security controls to reduce Council's exposure to cyber security risks.	

RISK TYPE: FINANCIAL	
Risk Appetite Statement	**Risk Tolerance Statement**
Council has a **LOW TO MODERATE RISK** appetite for risks related to financial management, focusing	Council will **NOT** tolerate:

on maintaining long-term financial sustainability while allowing for some flexibility to pursue opportunities to generate additional sources of income or reduce costs.	• risks that threaten the Council's financial viability or reputation; • failure to maintain or implement adequate systems, processes and controls which adequately prevent fraud; or • fraudulent actions or corrupt behaviour of employees or councillors.
Council Encourages	
• Foster employee awareness of the financial impact of their actions and decisions. • Encourage a culture of open communication and reporting on financial impacts and risks. • Make informed investment decisions based on sound financial analysis and forecasting. • Implement effective internal controls, including regular reporting on budget status and periodic budget reviews. • Reporting any Fraud and Corruption incidents in accordance with Council's policies	

RISK TYPE: ECONOMIC	
Risk Appetite Statement	**Risk Tolerance Statement**
Council has a **MODERATE RISK** appetite for risks related to economic development, with a focus on pursuing opportunities that support the community and long-term economic growth.	Council will **NOT** tolerate: • Risks that threaten the Council's financial or reputational sustainability; or • Council decisions that cause a sustained reduction in gross regional product
Council Encourages	
• Pursue opportunities that enhance the Council's economic resilience and prosperity through informed council decisions. • Foster engagement and partnership with the Council's business community for the benefit of the Island.	

RISK TYPE: POLITICAL / REPUTATIONAL RISK	
Risk Appetite Statement	**Risk Tolerance Statement**
Council has a **LOW TO MODERATE RISK** appetite for risks related to: Commonwealth, State and local political decision making misaligned with Council strategic and operational plans, policies and objectives, and Reputational damage or loss of public trust, with a focus on maintaining a positive public image and strong relationships with stakeholders.	Council will **NOT** tolerate: • risks that seriously harm Council's reputation or violate ethical or legal standards; • improper, unethical, corrupt, unprofessional behaviour or failure to act in accordance with Council's values and policies; • failure to act or make decisions in a fair, honest, transparent, and accountable manner; • failure to manage conflicts of interest; or • failure to respond to complaints professionally.
Council Encourages	
• Employees to engage with the community in a professional and respectful manner. • Reporting any ethical standards issues in all their interactions with stakeholders and members of the public.	

RISK TYPE: ASSETS	
Risk Appetite Statement	**Risk Tolerance Statement**
Council has a **LOW TO MODERATE RISK** appetite for risks related to asset management, with a focus on maintaining the integrity and functionality of critical assets while allowing for some flexibility to pursue opportunities for innovation and improvement.	Council will **NOT** tolerate: • risks that compromise the functionality or safety of critical assets or that threaten the Council's financial sustainability; • asset failure significantly earlier than the expected useful life of the asset; and • failure to promptly escalate critical damage to an insurance provider.
Council Encourages	
Good Asset Management practices to ensure the continuity and resilience of critical services and operations for the benefit of the community.	

RISK TYPE: SERVICE DELIVERY	
Risk Appetite Statement	**Risk Tolerance Statement**
Council has a **LOW TO MODERATE RISK** appetite for risks related to service delivery, focusing on maintaining adopted levels of service while allowing for some flexibility to pursue opportunities for innovation and improvement.	Council will **NOT** tolerate: • risks that compromise the safety or well-being of staff or community members or that threaten Council's reputation or financial sustainability; • failure to develop plans to respond to disruption and ensure continuity of critical business functions; or • failure to promptly escalate critical business impact or outages.
Council Encourages	
A culture that prioritises quality customer service, stakeholder engagement, and responsiveness, and recognises the importance of these values in building strong and positive relationships with the community ans stakeholders.	

8 RISK MANAGEMENT PROCESS

To ensure effective risk management, it is crucial that the process is integrated into Council's management, culture, and practices, tailored to our unique operational and business processes. As outlined in Figure 3 of the ISO 31000:2018 - Risk Management - Guidelines, the risk management process involves establishing the context, assessing the risk, treating the risk, monitoring the risk, and reviewing the risk. This comprehensive process needs to be effectively communicated to stakeholders, who should be consulted throughout the entire process to provide valuable input.

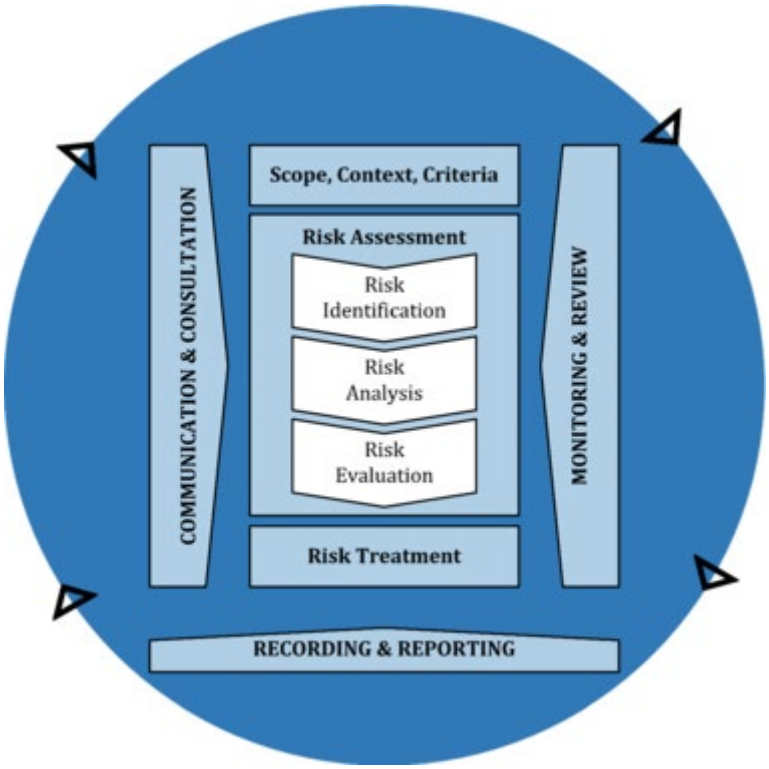

Figure 4: ISO 31000:2018 - Risk Management Process

Council's Risk Management Process offers a detailed framework for conducting a comprehensive risk assessment. This process sets out the specific thresholds for "likelihood" and "consequence," as determined by Council, as well as the Risk Rating Matrix, which enables a Risk Rating to be determined for each identified risk.

This process also guides users on the appropriate course of action depending on the inherent risk identified. For example, a risk with an Extreme Rating must receive immediate action and be reported to the General Manager. In contrast, a risk that has a Low rating may only require ongoing monitoring and no further treatment.

It is worth noting that the context establishment may be specific to each risk, and the key stakeholders involved will vary from one risk to another. Individuals from various levels of the organisation involved in the service delivery or identified activities must be included in the risk management process to ensure a comprehensive and practical approach.

9 INSURANCE

Council must optimise its available resources to effectively manage risk and minimise any potential loss to the community and its assets. Although insurance can be an effective tool for transferring or managing the risk of financial loss, it may not always be cost-beneficial or transferable.

When evaluating the use of insurance, several factors must be considered, including the nature of the risk, the availability of alternative risk management and mitigation strategies, the financial consequences of choosing not to insure, and the level of loss the Council is willing to absorb.

Responsible officers must ensure that they have the appropriate insurance in place for their specific risks. The level of insurance required should be based on tolerance levels, past claims experience, and the availability and cost of insurance. Officers must also consider Council's risk profile and determine the appropriate level of insurance required.

Preventative and mitigating measures should be thoroughly evaluated to reduce the probability or severity of an adverse risk event occurring. Even if the risk has been insured, it is still necessary to implement measures to manage the risk if it is deemed cost-benefit. The risk owner must document how the risk is to be managed via the risk register, regardless of whether the risk is insurable or not.

10 MONITORING AND REPORTING

The monitoring and evaluation of the Framework will be conducted on an annual basis by the Responsible Officer.

Council's reporting requirements are clearly defined and outlined in the *Risk Management Policy*.

11 REVIEW AND VERSION CONTROL

Policy Number:	2.13.00	**Responsible Officer:**	Governance Coordinator
Next Review Date:	June 2024		
Version:	**Resolution Number:**	**Effective Date:**	**Description:**
1.0	2018/148	19 September 2018	Developed and adopted
2.0	2023/55	07 June 2023	Updated and adopted